

物联网

安全技术

余智豪 马莉 胡春萍 编著

清华大学出版社

物联网安全技术

余智豪　马莉　胡春萍　编著

清华大学出版社
北　京

内 容 简 介

本书共分为 7 章，深入、全面、系统地分析了物联网安全中的系统结构、关键技术及其典型的解决方案。其中，第 1 章是物联网概述；第 2 章是物联网安全概述；第 3 章是信息安全技术基础；第 4 章是物联网感知层安全技术，分析了 RFID 安全技术、无线传感器网络安全技术和物联网终端安全；第 5 章是物联网网络层安全技术，分析了核心网安全技术、无线网络安全技术和移动通信系统安全；第 6 章是物联网应用层安全技术，分析了云计算安全、中间件安全、数据安全、隐私安全；第 7 章是物联网安全管理概述。

本书可作为物联网工程、信息安全、计算机科学等专业的研究生和高年级本科生教材，对从事信息和网络安全研究的科学工作者、从事物联网安全技术研究以及应用和管理的工程技术人员也具有一定的参考价值。

图书在版编目（CIP）数据

物联网安全技术/余智豪等编著. --北京：清华大学出版社，2016
ISBN 978-7-302-41999-0

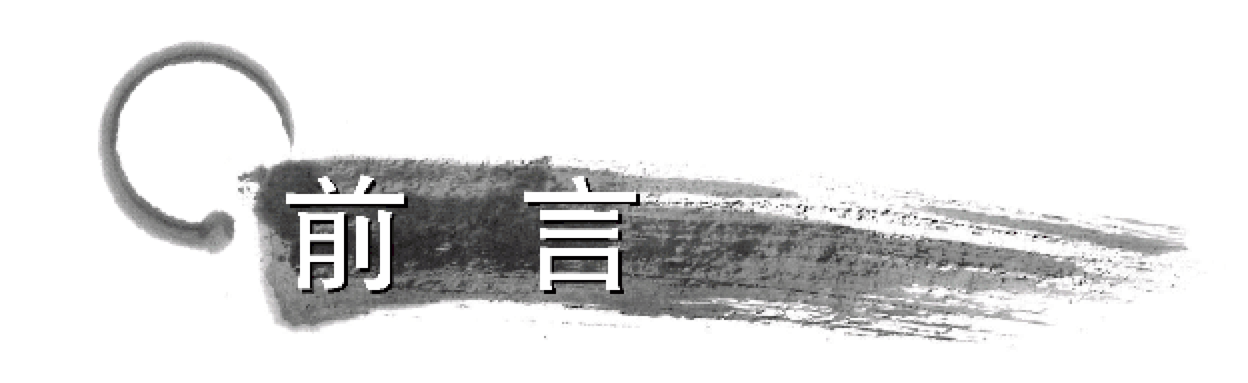
Ⅰ. ①物…　Ⅱ. ①余…　Ⅲ. ①互联网络－应用－安全技术－高等学校－教材 ②智能技术－应用－安全技术－高等学校－教材　Ⅳ. ①TP393.4 ②TP18

中国版本图书馆 CIP 数据核字(2015)第 263184 号

责任编辑：刘向威　李　晔
封面设计：
责任校对：李建庄
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：21.25　　**字　　数**：534 千字
版　　次：2016 年 4 月第 1 版　　**印　　次**：2016 年 4 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：060806-01



物联网技术的发展和应用能够给人们的工作和生活带来便利，可以大大提高工作效率和生活质量，推动国民经济的大力发展。但是，我们也必须清醒地认识到物联网的应用存在巨大的安全隐患，信息化与网络化带来的风险问题在物联网中变得更加迫切和复杂。因此，在物联网时代，安全问题面临前所未有的挑战，如何建立安全、可靠的物联网系统是摆在人们面前的迫切问题。

为此，本书注重于物联网安全的基础知识和典型应用，理论联系实际，比较全面地论述了物联网安全知识、技术体系和相关理论，对物联网安全的关键技术进行了详细的分析。在写作构思和内容编排上，本书的内容图文并茂、便于阅读，力求使读者在物联网安全方面打好扎实的基础，并且使读者不仅对物联网安全技术有比较清晰的理解和认识，还能够进一步深入地学习和掌握相关的知识。

本书面向的主要对象包括高等院校物联网工程、信息安全、计算机科学及相关专业的研究生和本科高年级学生、从事信息和网络安全研究的科学工作者、从事物联网安全应用和管理方面工作的工程技术人员等。

本书共分为 7 章，深入、全面、系统地分析了物联网安全领域中的系统结构、关键技术及其典型的解决方案。

第 1 章是物联网概述，简要地介绍了物联网的起源与发展、物联网的定义与特征、物联网的体系架构、物联网的关键技术、物联网的标准体系和物联网的典型应用等内容。

第 2 章是物联网安全概述，简要地介绍了物联网的安全特征、物联网安全体系结构、感知层安全概述、网络层安全概述和应用层安全概述等内容。

第 3 章是信息安全技术基础，主要介绍了密码学概论、常用加密技术、密码技术的应用和常用安全协议等内容。

第 4 章是物联网感知层安全技术，深入、详细地分析了 RFID 安全技术、无线传感器网络安全技术和物联网终端安全等内容。

第 5 章是物联网网络层安全技术，深入、详细地分析了核心网安全技术、无线网络安全技术和移动通信系统安全等内容。

第 6 章是物联网应用层安全技术，深入、详细地分析了云计算安全、中间件安全、数据安全、隐私安全、位置隐私保护、轨迹隐私保护等内容。

第 7 章是物联网安全管理概述，简要地介绍了物联网安全管理概述、信息安全标准化组织、信息安全管理模型、信息安全管理标准和物联网安全风险评估等内容。

本书具有如下特色：

① 内容新颖。本书紧扣物联网安全技术的发展方向，内容新颖、分析透彻、反映最新的主流技术。融入了国内外最新的物联网安全知识和最新的物联网安全的科研成果。

② 关键技术。本书全面、深入、系统地论述物联网安全的关键技术，包括 RFID 安全、

无线传感器网络安全、核心网安全、云计算安全、隐私安全等。

③ 结构严谨。提供清晰完整的知识体系，全书结构严谨，以物联网安全体系结构为基础，按照“从下层到上层的、从概括到深入”的原则进行编写，便于读者从总体上理解物联网安全的内涵。

④ 图文并茂。本书的内容由浅入深、易于理解，从具体的物联网安全技术应用案例讲起，图文并茂，力图将深奥的、复杂的理论转化为便于读者理解的知识。

⑤ 便于教学。为了方便教师的教学，随书还配备了教师授课用的、详细的教学课件(PowerPoint 文件)，其可以从清华大学出版社网站 www.tup.com.cn 下载。

本书由广东佛山科学技术学院的余智豪、马莉、胡春萍共同编著。余智豪编写了第 1 章、第 2 章、第 4 章、第 5 章和第 7 章的全部内容，还编写了第 6 章有关隐私安全的内容；马莉编写了第 3 章全部内容和第 6 章的关于云计算安全的内容；胡春萍编写了第 6 章的关于数据安全部分的内容。全书由余智豪策划、主编、审核、修改和定稿。

在本书的编写过程中，编者参考了国内外大量的物联网及计算机网络安全方面的文献、书刊、相关的网站等相关资料。在此，对所有的被参考和被引用的文献作者表示衷心的感谢。最后，还要感谢所有对本书的写作和出版提供了帮助的朋友。

由于编者的水平和学识有限，本书难免存在错误和不妥之处，恳请广大读者不吝赐教。

编　者

2016 年 1 月

目 录

第1章 物联网概述

1.1 物联网的起源与发展

首先，让我们描绘一下未来应用物联网技术的美好生活——

在将来的某一天，当你正在办公室里忙碌时，也许会担心在学校里上学的孩子的安全。针对这个问题，只要给孩子佩戴一块智能定位的手表，然后在你的手机或办公用的电脑的电子地图上设定一个边界，这样，一旦孩子的活动范围超出了限定的区域，手机或电脑就会自动地发出报警信号。冬天，当你忙碌了一整天，准备下班回家的时候，只要提前用手机简单地发出一条指令，就可以指挥停在户外的汽车化雪解冻；你还可以遥控家中的空调开始工作，遥控微波炉开始熬汤，遥控电饭锅开始煮饭；也许你在下班回家的路上买了一瓶美酒，只要简单地用手机扫描一下电子标签，就可以识别这瓶酒的真伪；当你的汽车快回到家门口时，车库就会聪明地认出了你，自动地为你打开大门；当你迈进客厅，电视自动播放你喜爱的节目……以上这些美好的设想，都可以用物联网技术轻易地实现。

美国微软公司总裁比尔·盖茨先生的智能家居，就是物联网技术应用的典型案例。这幢豪宅依山傍水，雄踞于美国华盛顿湖东岸，修建于20世纪90年代，从设计、施工到建成，整整花了七年时间，耗资6000万美元。整幢建筑物共铺设了长达80km的光纤和电缆，家中几乎所有的设施都通过网络连接在一起。大门外安装有天气感知器，可以根据各项天气指标通知户内的空调系统调节室内的温度和湿度，主人在回家途中只要用手机发布指令，家中的浴缸就开始放水调温，为主人洗澡做好准备。更为奇妙的是，每一位来访的客人都可以领到一个含有电子标签的胸针，胸针中存放了每位客人对灯光的亮度和颜色、电视频道、室内的通风、温度、湿度、音乐、绘画等的个人喜好。当客人走进某个房间时，电子标签就会通过传感系统与房间中的设备交换信息，让所有的设备自动地将环境调整到宾至如归的境界，使客人感到最舒适、最满意。

物联网的应用，可以大大改善我们的工作和生活，帮助我们更好地实现对一切智能物体的远程管理，让我们轻松地做到“运筹帷幄之中，决胜千里之外”。

早在1991年，美国麻省理工学院(MIT)的凯文·奥斯通教授(Kevin Ashton)，就已经首次提出了物联网的概念。

1995年，美国微软公司总裁比尔·盖茨先生在其著作《未来之路》一书中也提及了物联网，但是并没有引起人们的重视。

1999 年美国麻省理工学院(MIT)建立了自动识别中心(Auto-ID),提出"万物皆可通过网络互联",阐明了物联网的基本概念。早期的物联网是基于射频识别(RFID)技术的物流网络。

2004 年日本总务省(MIC)提出 u-Japan 计划,该战略力求实现人与人、物与物、人与物之间的连接,希望将日本建设成一个随时、随地、任何物体、任何人均可连接的泛在网络社会。

2005 年 11 月 17 日,在突尼斯举行的信息社会世界峰会(WSIS)上,国际电信联盟(ITU)发布《ITU 互联网报告 2005:物联网》,给出了"物联网"的定义。此时,物联网的定义和范围已经发生了变化,覆盖范围有了较大的拓展,不再只是指基于 RFID 技术的物联网。

2006 年韩国确立了 u-Korea 计划,该计划旨在建立无所不在的社会(ubiquitous society),在民众的生活环境里建设智能型网络(如 IPv6、BcN、USN)和各种新型应用(如 DMB、Telematics、RFID),让民众可以随时随地享有科技智慧服务。2009 年韩国通信委员会出台了《物联网基础设施构建基本规划》,将物联网确定为新增长动力,提出到 2012 年实现"通过构建世界最先进的物联网基础实施,打造未来广播通信融合领域超一流信息通信技术强国"的目标。

2009 年欧盟执委会发表了欧洲物联网行动计划,描绘了物联网技术的应用前景,提出欧盟政府要加强对物联网的管理,促进物联网的发展。

2009 年 1 月 28 日,IBM 首次提出"智慧地球"概念,建议美国政府投资新一代的智慧型基础设施。当年,美国将新能源和物联网列为振兴经济的两大重点。

2009 年 8 月,温家宝总理在无锡视察时提出"感知中国",无锡市率先建立了"感知中国"研究中心,中国科学院、运营商、多所大学在无锡建立了物联网研究院。物联网被正式列为国家五大新兴战略性产业之一,写入了十一届全国人大三次会议政府工作报告,物联网在中国受到了全社会极大的关注。

1.2 物联网的定义与特征

1.2.1 物联网的定义

关于物联网有许多种不同的定义。各个领域的专家和学者们都先后提出了自己的定义,众说纷纭、各抒己见。这些定义是专家和学者们分别从自己的研究角度提出来的。在本书中,笔者选择最具代表性的几种定义供读者们参考:

(1) 物联网是实现物体与物体连接的互联网络。英语中"物联网"一词为 Internet of Things(缩写为 IoT),可以翻译成物与物的互联网。

(2) 美国麻省理工学院的自动识别中心(Auto-ID)指出:物联网把所有的物品通过射频识别和条形码等信息传感设备,与互联网紧密地连接起来,实现智能化的识别和管理。

(3) 物联网是指将各种信息传感设备,如射频识别(RFID)装置、红外感应器、全球定位系统、激光扫描器与互联网结合起来。其目的是把所有物品连接在一起。

(4) 物联网经过接口与无线网络(也含固定网络),使物体与物体之间实现沟通和对话,以及使人与物体之间实现沟通与对话。

（5）中国电信对物联网的定义是：物联网是基于特定的终端，以有线或无线等接入手段，为集团和家庭客户提供机器到机器、机器到人的解决方案，满足客户对生产过程、家居生活监控、指挥调度、远程数据采集和测量、远程诊疗等方面的信息化需求。

以上几种对物联网的定义都具有一定的局限性，目前比较准确的是2005年国际电信联盟（ITU）给出的定义：物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备，按照约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

物联网有狭义与广义之分，狭义的物联网是指物与物之间的连接和信息交换；广义的物联网不仅包括物与物的信息交换，还包括人与物、人与人之间的广泛的连接和信息交换。广义的物联网是一种基于泛在网及其多制式、多系统、多终端等综合的网络。

在广义物联网中不仅是机器到机器（M2M），也包括机器到人（M2P）、人到人（P2P）、人到机器（P2M）之间广泛的通信和信息的交流。而在这个物联网中的机器（M），定义为可以获取信息的各种终端，它们包括各类传感器、RFID读写器、智能手机、PC、平板电脑、摄像头、电子望远镜、GPS等。

总之，物联网可以感知到人类需要的各种信息终端（即传感器），这些信息终端都被连接到泛在网上。这里所说的泛在网，几乎囊括了当代各种信息通信网络，不仅仅包括固定的互联网和移动的互联网，还包括如电信固定网、无线移动网、广播电视网和各种其他专用网络。并靠这些网络的整合将各种智能终端与人紧密联系在一起，构成了一个任何时间、任何地点都可以取得任何服务的物联网。物联网的最终目的是为人类提供各种现代化服务。

1.2.2　物联网的特征

根据物联网实现的功能来进行分析，物联网具备以下的四个特征：

1. 全面感知

全面感知是指利用RFID、无线传感器、条形码、二维码等识别设备随时随地获取物体的信息；

2. 可靠传输

可靠传输是指通过各种接入网络与互联网的融合，将物体的信息实时、可靠、准确地传输；

3. 智能处理

智能处理是指利用云计算、模糊识别等各种智能计算技术，对海量的物体信息进行分析和处理，对物体实施智能化的控制；

4. 综合应用

综合应用是根据各个行业、各种业务的具体特点，形成各种单独的业务应用，或者整个行业及系统的建设应用方案。

1.3 物联网的体系结构

物联网的体系结构如图 1-1 所示。

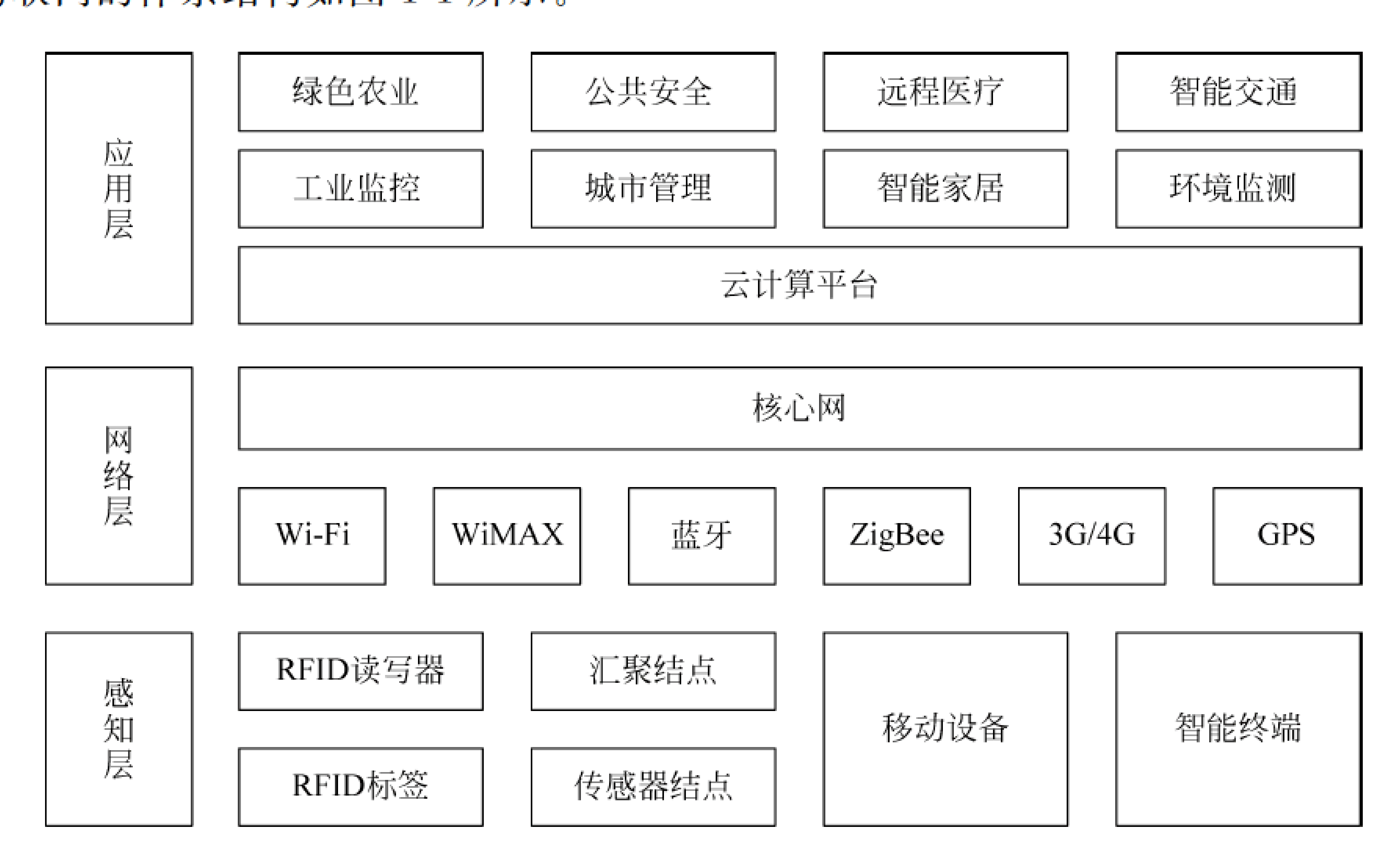


图 1-1 物联网体系架构

到目前为止，物联网的体系结构还没有统一的标准。在本书中，我们采用业界公认的物联网体系结构，分为三个层次：感知层、网络层、应用层。

1.3.1 感知层

感知层由传感器结点和接入网关等组成，传感器感知外部世界的温度、湿度、声音和图像等信息，并传送到上层的接入网关，由接入网关将收集到的信息通过网络层提交到后台处理。当后台对数据处理完毕后，发送执行命令到相应的执行机构，完成对被控对象或被测对象的控制参数调整，或者发出某种信号以实现远程监控。

感知层是物联网技术发展和应用的基础，涉及 RFID、近距离无线通信、传感器技术、无线传感网等技术。

射频识别技术（Radio Frequency Identification，RFID），又称为无线射频识别，这是一种近距离通信技术，通过无线电讯号识别特定目标并读写相关数据，而不需要识别系统与特定目标之间建立机械或光学接触。RFID 常用的工作频率可分为低频（125k～134.2kHz）、高频（13.56MHz）、超高频和微波等。RFID 读写器也分为移动式和固定式两类。RFID 技术的应用很广，例如：图书馆、门禁系统、食品安全等领域。

粘贴或者安装在物品上的 RFID 标签，以及用来识别 RFID 信息的读写器等，都属于物联网的感知层。在感知层中，被检测的信息是 RFID 标签中与它所粘贴的物品对应的物品身份标识。高速公路不停车收费系统、超市仓储管理系统等都是 RFID 典型的应用案例。

近距离无线通信技术（Near Field Communication，NFC）是一种短距离的高频无线通信技术，允许电子设备之间进行非接触式点对点数据传输，在 10cm（3.9 英寸）内，交换数据。

NFC 技术由免接触式射频识别(RFID)演变而来,由飞利浦公司和索尼公司共同开发的 NFC 是一种非接触式识别和互联技术,可以在移动设备、消费类电子产品、PC 和智能控件工具间进行近距离无线通信。

近距离无线通信是一种短距离高频的无线电技术,在 13.56MHz 频率运行于 20 厘米距离内。其传输速度有 106kbps、212kbps 或 424kbps 三种。目前近场通信已通过成为 ISO/IEC IS 18092 国际标准、EMCA-340 标准与 ETSI TS 102 190 标准。NFC 采用主动和被动两种读取模式。

传感器技术是实现测试与自动控制的重要环节。在物联网感知层中,传感器的主要特征是能准确传递和检测出被测对象某一形态的信息,并将其转换成另一形态的信息。具体地说传感器是指那些对被测对象的某一确定的信息具有感受(或响应)与检出功能,并使之按照一定规律转换成与之对应的可输出信号的元器件或装置。如果没有传感器对被测对象的原始信息进行准确可靠地捕获和转换,一切准确的测试与控制都将无法实现。

传感器网络实现了数据的采集、处理和传输三种功能。它与通信技术和计算机技术共同构成信息技术的三大支柱。

无线传感器网络(Wireless Sensor Network, WSN)是由大量的静止或移动的传感器以自组织和多跳的方式构成的无线网络,以协作地感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息,并最终把这些信息发送给物联网的所有者。

无线传感器网络所具有的众多类型的传感器,可探测包括地震、电磁、温度、湿度、噪声、光强度、压力、土壤成分、移动物体的大小、速度和方向等周边环境中多种多样的现象。潜在的应用领域可以归纳为:军事、航空、防爆、救灾、环境、医疗、保健、家居、工业、商业等领域。

1.3.2 网络层

在物联网的体系架构中,网络层位于中间,它向下与感知层相连接,向上则与应用层相连接,高效、稳定、实时、安全地传输上层与下层之间的数据。

网络层是物联网的神经中枢和大脑。实现信息传递和处理。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等。网络层将感知层获取的信息进行传递和处理,类似于人体结构中的神经中枢和大脑。

网络层的主要功能是传输和预处理感知层所获得的数据。这些数据可以通过移动通信网、互联网、企业内部网、各类专线网、局域网、城域网等进行传输。特别是在三网(有线电话网、有线电视网、光纤网)融合后,有线电视网也能承担物联网网络层的功能,有利于物联网的加快推进。网络层所需要的关键技术包括核心网技术、近距离无线网络技术和移动通信技术等。

物联网的网络层是建立在现有的互联网等通信网络的基础上的。物联网通过各种接入设备与互联网相连。例如手机付费系统中由刷卡设备将内置手机的 RFID 信息采集上传到互联网,网络层完成后台鉴权认证,并从银行网络划账。

网络层中的感知数据管理与处理技术是实现以数据为中心的物联网的核心技术,包括传感网数据的存储、查询、分析、挖掘和理解,以及基于感知数据决策的理论与技术。

1.3.3 应用层

应用层位于物联网体系结构的最上层。应用层与各种不同的行业相结合，实现广泛智能化。应用层是物联网与行业专业技术的深度融合，与行业需求结合，实现行业智能化，这类似于人的社会分工，最终构成人类社会。

在各层之间，信息不是单向传递的，也有交互、控制等，所传递的信息多种多样，这其中关键是物品的信息，包括在特定应用系统范围内能唯一标识物品的识别码和物品的静态与动态信息。

云计算平台作为海量感知数据的存储、分析平台，将是物联网的重要组成部分，也是应用层众多应用的基础。在产业链中，通信网络运营商和云计算平台提供商将在物联网中占据重要的地位。

应用层主要是根据行业特点，借助物联网的技术手段，开发各类的行业应用解决方案，将物联网的优势与行业的生产经营、信息化管理、组织调度结合起来，形成各类的物联网解决方案，构建智能化的行业应用。如交通行业，涉及的就是智能交通技术；电力行业采用的是智能电网技术，物流行业采用的是智慧物流技术等。物联网在各行业的应用还涉及系统集成技术、资源打包技术等。

物联网应用层利用经过分析处理的感知数据，为各行业的用户提供丰富的特定服务。物联网的应用可分为监控型(物流监控、污染监控)、查询型(智能检索、远程抄表)、控制型(智能交通、智能家居、路灯控制)、扫描型(手机钱包、高速公路不停车收费)等。

应用层是物联网发展的目的，软件开发、智能控制技术将会为用户提供丰富多彩的物联网应用。各种行业和家庭应用的开发将会推动物联网的普及，也给整个物联网产业链带来利润。

1.4 物联网的关键技术

1.4.1 RFID 技术

射频识别(Radio Frequency IDentification，RFID)是一种无线通信技术，可以通过无线电信号识别特定目标并读写相关数据，而无须识别系统与特定目标之间建立机械或者光学接触。

无线电的信号是通过调成无线电频率的电磁场，把数据从附着在物品上的电子标签上传送出去，以自动辨识与追踪该物品。某些电子标签在工作时，能够从读写器发出的电磁场中得到能量，并不需要电池；也有些电子标签本身配有电源，并可以主动发出无线电波(调成无线电频率的电磁场)。标签包含了电子存储的信息，在几米之内都可以被读写器识别。与条形码不同的是，RFID 标签不需要处在读写器视线范围之内，也可以嵌入被追踪物体之内。

RFID 系统结构图如图 1-2 所示。

从系统结构上分析，一套完整的 RFID 系统，由电子标签、读写器、中间件和应用软件等

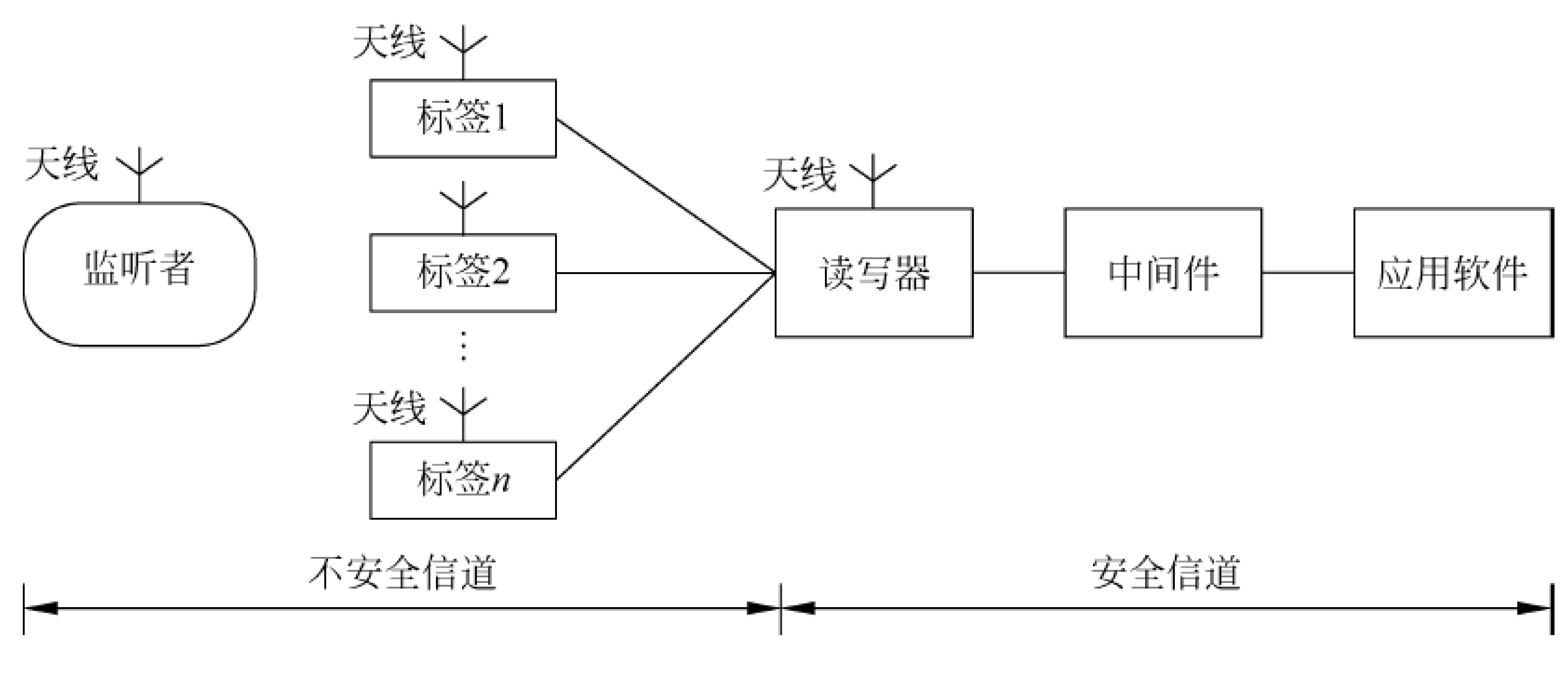


图 1-2 RFID 系统结构图

部分组成。

1. 电子标签

电子标签由天线、耦合元件及芯片组成，在 RFID 系统中，通常都用标签作为物品的应答器，每个电子标签具有唯一的电子编码，粘贴或附着在物体上，用于标识物品。天线(Antenna)是将 RFID 标签的数据信息传递给阅读器的设备。RFID 天线可分为标签天线和阅读器天线两种类型。

2. 读写器

读写器由天线、耦合元件和芯片组成，是读取(也可以写入)标签信息的设备，可设计为手持式或固定式。读写器(Reader)发射某一特定频率的无线电波，将能量传送给标签，用以驱动电子标签中电路，将其内部的数据送出，此时读写器便按照次序接收这些数据，并送给中间件做相应的处理。

3. 中间件

中间件(Middleware)位于读写器与应用软件的中间，它是一种面向消息的、可以接受应用软件端发送的请求，并同时与一个或者多个读写器交互通信，在接收数据和处理数据后向应用软件返回处理结果的特殊软件。

4. 应用软件

顾名思义，应用软件是工作在应用层的软件，它主要是把收集的数据进一步处理，并为人们所使用。应用软件系统是计算机后台处理系统，计算机通过有线或无线网络与阅读器相连，获取电子标签的内部信息，对读取的数据进行筛选和分析，并进行后台处理。

RFID 技术的基本工作原理并不复杂：标签进入磁场后，接收解读器发出的射频信号，凭借感应电流所获得的能量，并发送存储在芯片中的产品信息(Passive Tag，无源标签或被动标签)，或者由标签主动发送某一频率的信号(Active Tag，有源标签或主动标签)，读写器读取信息并解码后，送至计算机系统进行有关数据处理。

以 RFID 读写器与电子标签之间的通信及能量感应方式来划分，大致上可以分成感应

耦合式(Inductive Coupling)及后向散射耦合式(Backscatter Coupling)两种。一般低频的RFID采用第一种方式,而较高频的RFID大多采用第二种方式。

根据使用的结构和技术不同,读写器可以是读出设备,也可以是读/写设备,它是RFID系统信息控制和处理中心。读写器通常由耦合模块、收发模块、控制模块和接口单元组成。读写器和电子标签之间一般采用半双工通信方式进行信息交换,同时读写器通过耦合给无源的电子标签提供能量和时序。在实际应用中,进一步通过以太网(Ethernet)或无线局域网(WLAN)等实现对物体识别信息的采集、处理及远程传送等管理功能。

许多行业都可以应用射频识别技术。例如:将RFID电子标签粘贴在一辆正在生产过程中的汽车上,生产厂家便可以追踪此车的生产进度;将电子标签粘贴在产品上,仓库可以追踪产品所在的位置;将电子标签附于牲畜与宠物上,可以方便对牲畜与宠物的身份识别;RFID身份识别也可以使企业员工能够进入紧闭的大门;汽车上的RFID标签可以用于自动缴交收费路段或停车场的费用。

1.4.2 无线传感器网络技术

无线传感器网络(Wireless Sensor Network,WSN)简称为无线传感网,它是由大量的静止或移动的传感器以自组织和多跳的方式构成的无线网络,以协作地感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息,并最终把这些信息发送给网络的所有者。

无线传感网具有众多不同类型的传感器,可以探测包括地震、电磁、温度、湿度、噪声、光强度、压力、土壤成分、移动物体的大小、速度和方向等周边环境中多种多样的物理现象。潜在的应用领域可以归纳为:军事、航空、防爆、救灾、环境、医疗、保健、家居、工业、商业等领域。

1. 无线传感网的定义

无线传感网是由部署在监测区域内大量的廉价微型传感器结点组成的,通过无线通信方式形成的一个多跳的自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息,并发送给观察者。传感器、感知对象和观察者构成了无线传感器网络的三个要素。

近年来,微机电系统(Micro-Electro-Mechanism System,MEMS)、片上系统(System on Chip,SoC)、无线通信和低功耗嵌入式技术的飞速发展,孕育出无线传感器网络(Wireless Sensor Networks,WSN),并以其低功耗、低成本、分布式和自组织的特点带来了信息感知的一场变革。无线传感网就是由部署在监测区域内大量的廉价微型传感器结点组成,通过无线通信方式形成的一个多跳自组织网络。

正如互联网使计算机能够访问各种数字信息,而可以不管其保存到什么地方,传感器网络将能扩展人们与现实世界进行远程交互的能力。它甚至被人称为一种全新类型的计算机系统,这就是因为它区别于过去硬件的可到处散布的特点以及集体分析能力。

2. 无线传感网的结构

无线传感器网的结构如图1-3所示。

无线传感网系统通常包括传感器结点(Sensor)、汇聚结点(Sink)和任务管理结点

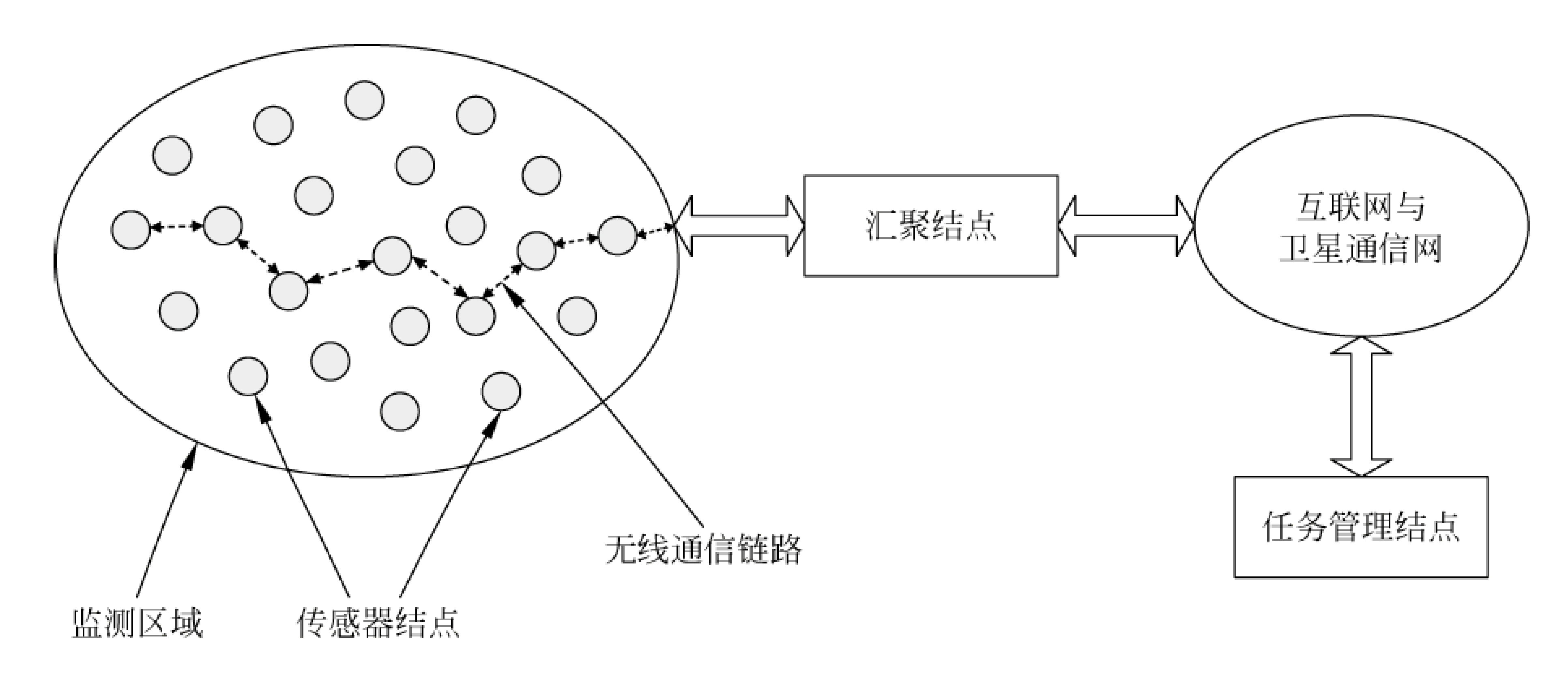


图 1-3　无线传感网的结构

(Coordinator)。

大量传感器结点随机部署在监测区域内部或附近,能够通过自组织方式构成网络。传感器结点监测的数据沿着其他传感器结点逐跳地进行传输,在传输过程中监测数据可能被多个结点处理,经过多跳后路由到汇聚结点,最后通过互联网或卫星到达管理结点。用户通过管理结点对传感器网络进行配置和管理,发布监测任务以及收集监测数据。

1) 传感器结点

传感器结点处理能力、存储能力和通信能力相对较弱,通过小容量电池供电。从网络功能上看,每个传感器结点除了进行本地信息收集和数据处理外,还要对其他结点转发来的数据进行存储、管理和融合,并与其他结点协作完成一些特定任务。

2) 汇聚结点

汇聚结点的处理能力、存储能力和通信能力相对较强,它是连接传感器网络与 Internet 等外部网络的网关,实现两种协议间的转换,同时向传感器结点发布来自管理结点的监测任务,并把 WSN 收集到的数据转发到外部网络上。汇聚结点既可以是一个具有增强功能的传感器结点,有足够的能量供给和更多的、Flash 和 SRAM 中的所有信息传输到计算机中,通过汇编软件,可很方便地把获取的信息转换成汇编文件格式,从而分析出传感结点所存储的程序代码、路由协议及密钥等机密信息,同时还可以修改程序代码,并加载到传感结点中。

3) 任务管理结点

任务管理结点用于动态地管理整个无线传感器网络。无线传感网的所有者通过管理结点访问无线传感器网络的资源。

1.4.3　M2M 技术

M2M 是"机器对机器通信(Machine to Machine)"或者"人对机器通信(Man to Machine)"的简称,主要是指通过"通信网络"传递信息从而实现机器对机器或人对机器的数据交换,也就是通过通信网络实现机器之间或人与机器之间的互联、互通。移动通信网络由于其网络的特殊性,终端侧不需要人工布线,可以提供移动性支撑,有利于节约成本,并可以满足在危险环境下的通信需求,使得以移动通信网络作为承载的 M2M 服务得到了业界的广泛关注。

M2M 平台的结构如图 1-4 所示。

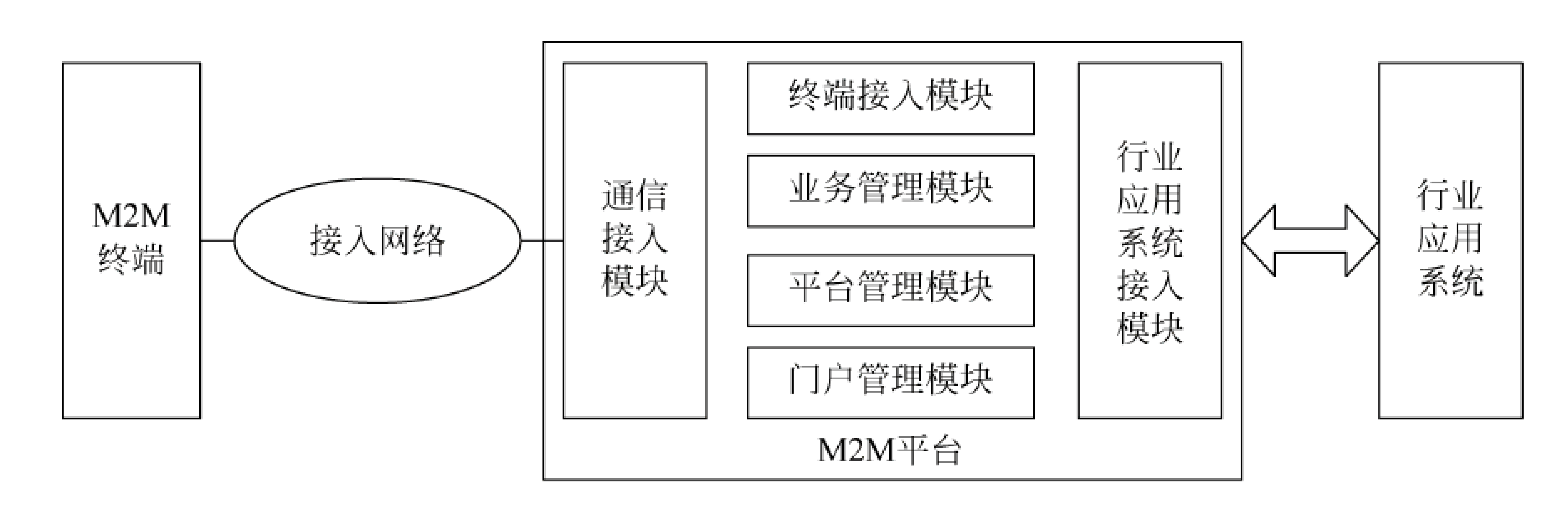


图 1-4 M2M 平台的结构

通信接入模块主要实现平台与 M2M 终端的通信连接,包括实现各种有线、无线接入网络的通信功能,如 2G/3G/LTE、Wi-Fi/WiMAX、ADSL 等。

终端接入模块主要实现平台对终端接入的认证管理、连接保持以及流量控制功能。在终端接入时,通过平台可以完成包括报文收发、报文认证、终端流控和协议适配的功能;在终端接入后,平台将完成终端注册、终端登录、终端退出以及终端注销等功能。此外终端接入模块还实现终端信息查询、状态监测、故障管理、参数查询和配置、远程控制和终端操作任务管理等功能。该模块中需要实现不同运营商的 M2M 终端接入协议,如中国移动通信企业标准无线机器通信协议(WMMP)、中国电信技术规范 M2M 终端监测控制协议(MDMP),以实现与 M2M 终端数据交互。

业务管理模块实现对终端和应用的基本信息的维护,对相应的行业应用业务进行受理、计费以及下单等。

平台管理模块主要完成 M2M 业务系统正常运行所需的基础数据管理、操作员账号管理、系统安全管理等功能。

门户管理模块提供人性化的 Web 登录界面,供平台管理员、业务管理员、企业客户、终端厂商、服务提供商等完成终端管理、应用管理、系统管理等功能。

行业应用系统接入模块实现平台与行业应用系统的对接,为行业应用系统提供终端管理服务和行业应用数据转发服务,包括应用接入的建立和维护、流量控制、终端管理请求处理以及应用数据转发请求处理等基本功能。

由以上分析可以看出,M2M 平台涉及的技术主要包括门户管理技术、通信接入技术、安全管理技术、流量控制技术和数据库管理技术等。

M2M 与社会的发展和人们的生活、工作密切相关,应用遍布各个领域,主要包括:交通领域(交通监控、定位导航)、电力领域(远程抄表和负载监控)、农业领域(大棚监控、动物溯源)、智慧城市(电梯监控、路灯控制)、安全领域(城市和企业安防)、环保领域(污染监控、水土检测)和智能家居(老人/小孩看护、智能安防)等。

1.4.4 基于 IPv6 协议的下一代互联网

1. IPv6 的基本概念

基于 IPv6 协议的下一代互联网是物联网的核心网络。IPv6 是英文 Internet Protocol

Version 6 的缩写，即互联网协议第 6 版。IPv6 是互联网工程任务组(Internet Engineering Task Force，IETF)设计的用于替代现行版本 IP 协议(IPv4)的下一代 IP 协议。

目前互联网广泛使用的 IPv4 技术，最大问题是网络地址资源有限，从理论上讲，编址 1600 万个网络、40 亿台主机。但采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数目大打折扣，以至 IP 地址已于 2011 年 2 月 3 日分配完毕。其中北美占有 3/4，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国截至 2010 年 6 月 IPv4 地址数量达到 2.5 亿，落后于 4.2 亿网民的需求。地址不足，严重地制约了中国及其他国家互联网的应用和发展。

一方面是地址资源数量的限制，另一方面是随着电子技术及网络技术的发展，物联网将进入人们的日常生活，身边的每一样东西都有可能需要连入物联网。在这样的环境下，IPv6 应运而生。单从数量级上来说，IPv6 所拥有的地址容量是 IPv4 的约 7.92×10^{28} 倍，达到 2^{128} 个。这不但解决了网络地址资源数量的问题，同时也为除电脑外的设备连入互联网在数量限制上扫清了障碍。

如果说 IPv4 实现的只是人机对话，而 IPv6 则扩展到任意事物之间的对话，它不仅可以为人类服务，还将服务于众多硬件设备，如家用电器、传感器、远程照相机、汽车等，它将是无时不在，无处不在的深入社会每个角落的真正的物联网。而且它所带来的经济效益将非常巨大。

2. IPv6 技术的优势

与 IPv4 技术相比，IPv6 技术具有以下几个优势：

1) IPv6 具有更大的地址空间

IPv4 中规定 IP 地址长度为 32，最大地址个数为 2^{32}；而 IPv6 中 IP 地址的长度为 128，即最大地址个数为 2^{128}。与 32 位地址空间相比，其地址空间增加了 $2^{128}-2^{32}$ 个。

目前，IPv4 采用 32 位二进制数地址长度，约有 43 亿个地址，而 IPv6 采用 128 位二进制数地址长度，具有海量的地址资源。地址的丰富将完全删除在 IPv4 互联网应用上的种种限制。

以智慧家庭为例，家中每一个传感器、每一台家电都可以有一个独立的 IP 地址，可以真正形成一个智慧家庭。

由于 IPv6 在地址空间上的优势，在很大程度上解决了 IPv4 互联网存在的问题，这也成为国际互联网从 IPv4 向 IPv6 演进的重要动力。

2) IPv6 使用更小的路由表

IPv6 的地址分配一开始就遵循聚类(Aggregation)的原则，这使得路由器能在路由表中用一条记录(Entry)表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。

3) 增强了对多媒体应用的支持

IPv6 增加了增强的组播(Multicast)支持以及对流的控制(Flow Control)，这使得基于 IPv6 的网络在多媒体应用方面有良好发展的前景，为服务质量(Quality of Service，QoS)控制提供了良好的网络平台。

4) 对自动配置(Auto Configuration)的支持

IPv6 技术增加了对自动配置(Auto Configuration)的支持。这是对动态主机配置协议

(Dynamic Host Configuration Protocol,DHCP)的改进和扩展,使得网络(尤其是局域网)的管理更加方便和快捷。

5）IPv6 具有更高的安全性

在使用 IPv6 网络中用户可以对网络层的数据进行加密并对 IP 报文进行校验,在 IPv6 中的加密与鉴别选项提供了分组的保密性与完整性。极大地增强了网络的安全性。

6）允许扩充

如果新的技术或应用需要时,IPv6 允许协议进行扩充。

7）更好的头部格式

IPv6 使用新的头部格式,其选项与基本头部分开,如果需要,可将选项插入到基本头部与上层数据之间。这就简化和加速了路由选择过程,因为大多数的选项不需要由路由选择。

8）实现附加的功能

IPv6 可以通过一些新的选项来实现附加的功能。

3. IPv6 的关键技术

1）IPv6 DNS 技术

IPv6 DNS 体系结构与 IPv4 DNS 体系结构相同,都是统一地采用树状型结构的域名空间。在从 IPv4 向 IPv6 的演进阶段,正在访问的域名可以对应于多个 IPv4 和 IPv6 地址,未来,随着 IPv6 网络的普及,IPv6 地址将逐渐取代 IPv4 地址。

2）IPv6 路由技术

IPv6 路由查找与 IPv4 的原理一样,是最长的地址匹配原则,选择最优路由还允许地址过滤、聚合、注射操作。原来的 IPv4IGP 和 BGP 的路由技术,如 RIP、ISIS、OSPFv2 和 BGP-4 等动态路由协议都可以一直延续到 IPv6 网络中,使用新的 IPv6 协议,新的版本分别是 RIPng、ISISv6、OSPFv3、BGP4＋。

3）IPv6 安全技术

与 IPv4 相比,IPv6 并没有提供新的安全技术,但 IPv6 协议可以通过 128 字节的 IPsec 报文头包、ICMP 地址解析和其他安全机制来提高安全性。

1.4.5 无线通信网络

无线通信网络包括无线局域网 Wi-Fi、无线城域网 WiMAX、ZigBee、蓝牙、红外通信、4G 移动通信等技术。

Wi-Fi 技术是通过在互联网连接基础上,安装无线访问点来实现的。这个访问点将无线信号通过短距离进行传输,一般仅覆盖 100 米。当一台支持 Wi-Fi 的设备(例如智能手机)遇到一个热点时,这个设备可以用无线方式连接到那个网络。大部分热点都位于供大众访问的地方,例如机场、咖啡店、旅馆、书店以及校园等等。许多家庭和办公室也拥有 Wi-Fi 网络。虽然有些热点是免费的,但是大部分稳定的公共 Wi-Fi 网络是由私人互联网服务提供商(ISP)提供的,因此会在用户连接到互联网时收取一定费用。

全球微波互联接入(Worldwide Interoperability for Microwave Access,WiMAX),也称为无线城域网或 802.16。WiMAX 是一项新兴的宽带无线接入技术,能提供面向互联网的高速连接,数据传输距离最远可达 50km。WiMAX 还具有 QoS 保障、传输速率高、业务丰

富多样等优点。WiMAX 技术的起点较高，它采用了代表未来通信技术发展方向的 OFDM/OFDMA、AAS、MIMO 等先进技术，随着 WiMAX 技术的发展，可以逐步实现宽带业务的移动化，而 3G 则实现移动业务的宽带化，两种网络的融合程度会越来越高。WiMAX 系统的结构如图 1-5 所示。

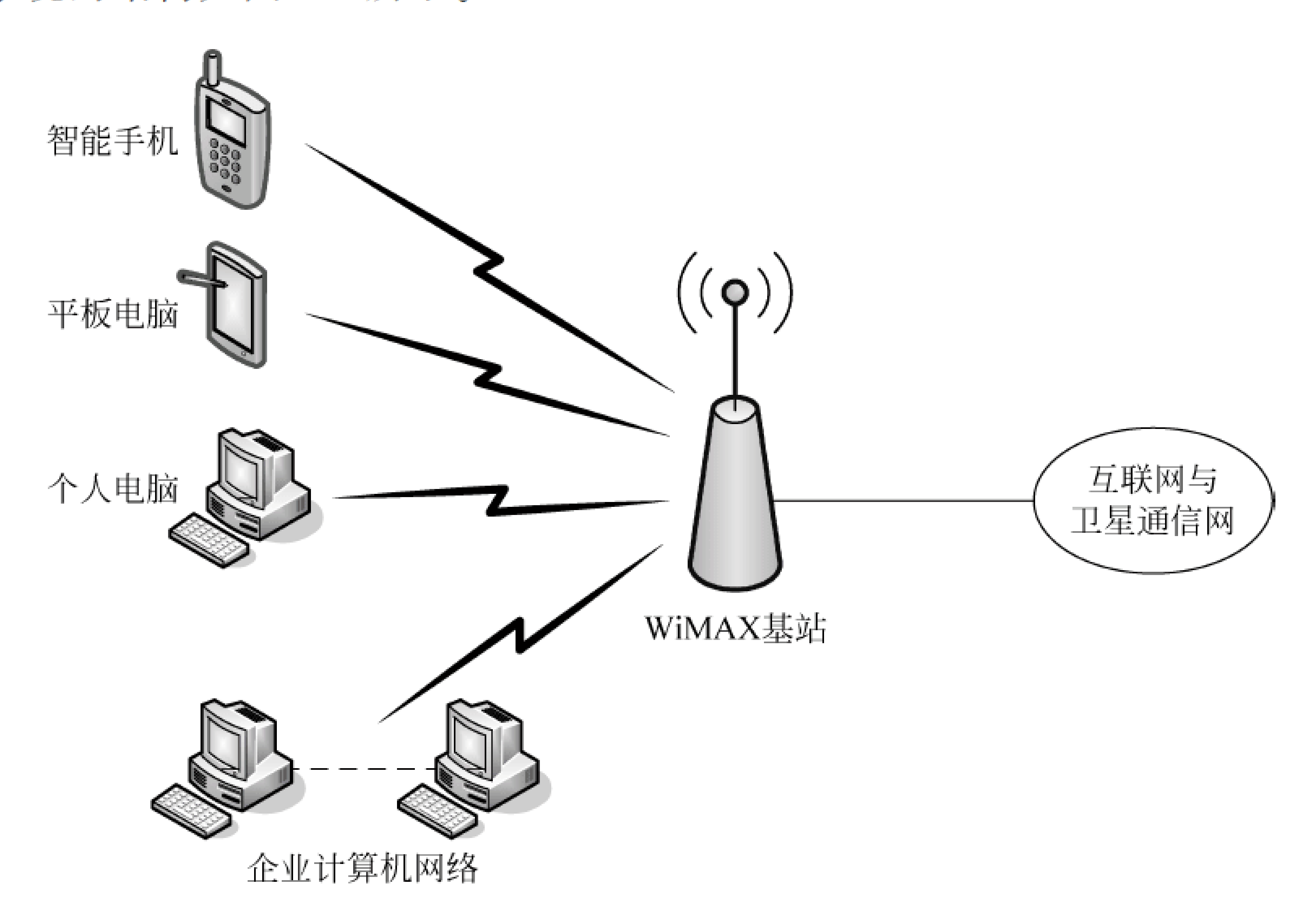


图 1-5　WiMAX 系统的结构

ZigBee 技术是一种近距离、低复杂度、低功耗、低速率、低成本的双向无线通信技术。主要用于距离短、功耗低且传输速率不高的各种电子设备之间进行数据传输以及典型的有周期性数据、间歇性数据和低反应时间数据传输的应用。与移动通信的 CDMA 网或 GSM 网不同的是，ZigBee 网络主要是为工业现场自动化控制数据传输而建立，因而，它必须具有简单、使用方便、工作可靠、价格低的特点。而移动通信网主要是为语音通信而建立，每个基站价值一般都在百万元人民币以上，而每个 ZigBee“基站”却不到 1000 元人民币。每个 ZigBee 网络结点不仅本身可以作为监控对象，例如其所连接的传感器直接进行数据采集和监控，还可以自动中转别的网络结点传过来的数据资料。除此之外，每一个 ZigBee 网络结点(FFD)还可在自己信号覆盖的范围内，和多个不承担网络信息中转任务的孤立的子结点(RFD)无线连接。

蓝牙，是一种支持设备短距离通信(一般 10m 内)的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与 Internet 之间的通信，从而使数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM (即工业、科学、医学)频段。其数据速率为 1Mbps。采用时分双工传输方案实现全双工传输。

红外通信技术利用 950nm 近红外波段的红外线作为传递信息的媒体，即通信信道。简而言之，红外通信的实质就是对二进制数字信号进行调制与解调，以便利用红外信道进行传输；红外通信接口就是针对红外信道的调制解调器。发送端将基带二进制信号调制为一系

列的脉冲串信号，通过红外发射管发射红外信号。接收端将接收到的红外信号转换成电信号，再经过放大、滤波等处理后送给解调电路进行解调，还原为二进制数字信号后输出。常用的有通过脉冲宽度来实现信号调制的脉宽调制(PWM)和通过脉冲串之间的时间间隔来实现信号调制的脉时调制(PPM)两种方法。

4G移动通信网络，是采用第四代移动通信技术的网络，英文缩写为4G。该技术包括TD-LTE和FDD-LTE两种制式。严格意义上来说，4G只是3.5G，LTE尽管被宣传为4G无线标准，但它其实并未被3GPP认可为国际电信联盟所描述的下一代无线通信标准IMT-Advanced，因此在严格意义上其还未达到4G的标准。只有升级版的LTE Advanced才满足国际电信联盟对4G的要求。4G集3G与WLAN于一体，能够快速传输数据、高质量、音频、视频和图像等。4G能够以高达100M bps的速度下载数据，比目前基于电话线的xDSL(2～6M bps)接入方式快20倍，并能够满足几乎所有用户对于无线服务的要求。此外，4G可以在DSL和有线电视调制解调器没有覆盖的地方部署，然后再扩展到整个地区。很明显，4G有着不可比拟的优越性。

1.4.6 GPS全球定位技术

GPS即全球定位系统(Global Positioning System，GPS)，是具有海、陆、空全方位实时三维导航与定位能力的卫星导航与定位系统。

GPS全球定位系统是由空间星座、地面控制和用户设备等三部分构成的。GPS技术能够快速、高效、准确地提供点、线、面要素的精确三维坐标以及其他相关信息，具有全天候、高精度、自动化、高效益等显著特点，广泛应用于军事、民用交通(船舶、飞机、汽车等)导航、大地测量、摄影测量、野外考察探险、土地利用调查、精确农业以及日常生活(人员跟踪、休闲娱乐)等不同领域。

GPS与现代通信技术相结合，使得测定地球表面三维坐标的方法从静态发展到动态，从数据后处理发展到实时的定位与导航，极大地扩展了它的应用广度和深度。载波相位差分法GPS技术可以极大提高相对定位精度，在小范围内可以达到厘米级精度。此外由于GPS测量技术对测点间地通视和几何图形等方面的要求比常规测量方法更加灵活、方便，已完全可以用来施测各种等级的控制网。

目前，全球的GPS系统有四个：美国的全星球导航定位系统、欧盟的伽利略卫星定位系统、俄罗斯的格洛纳斯卫星定位系统和中国的北斗卫星定位系统。

GPS全球定位系统的结构如图1-6所示。GPS全球定位系统包括三大部分：GPS卫星星座、地面监控系统和GPS信号接收机。

1. GPS卫星星座

由21颗工作卫星和3颗在轨备用卫星组成GPS卫星星座记作(21+3)GPS星座。24颗卫星均匀分布在6个轨道平面内轨道倾角为55°各个轨道平面之间相距60°，即轨道的升交点赤经各相差60°。每个轨道平面内各颗卫星之间的升交角距相差90°一轨道平面上的卫星比西边相邻轨道平面上的相应卫星超前30°。

在两万千米高空的GPS卫星，当地球对恒星来说自转一周时它们绕地球运行2周即绕地球一周的时间为12恒星时。这样对于地面观测者来说每天将提前4分钟见到同一颗

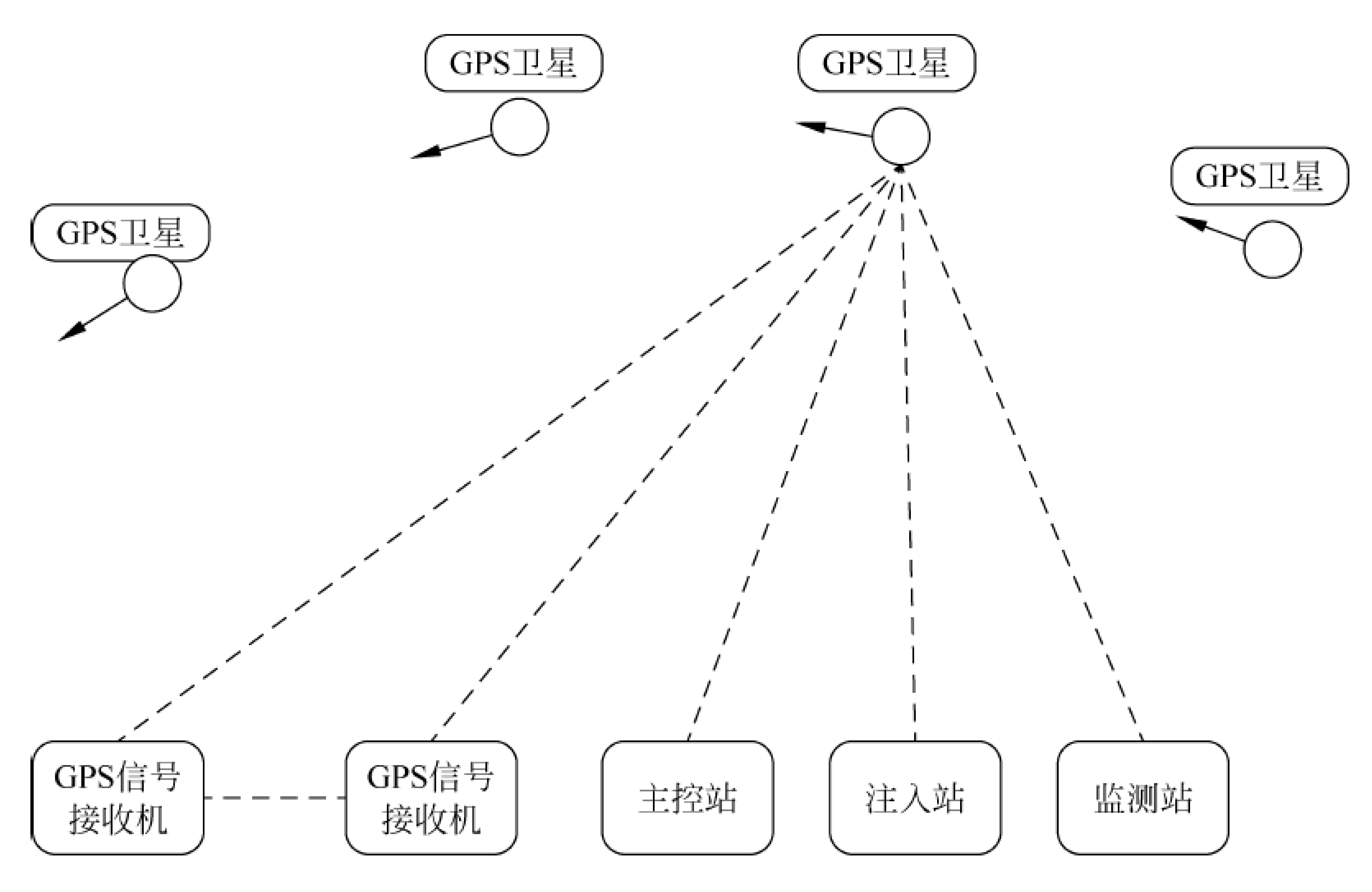


图 1-6　GPS 卫星定位系统的结构

GPS 卫星。位于地平线以上的卫星颗数随着时间和地点的不同而不同，最少可见到 4 颗，最多可见到 11 颗。在用 GPS 信号导航定位时，为了结算测站的三维坐标必须观测 4 颗 GPS 卫星，称为定位星座。这 4 颗卫星在观测过程中的几何位置分布对定位精度有一定的影响。对于某地某时甚至不能测得精确的点位坐标，这种时间段叫做“间隙段”。但这种时间间隙段是很短暂的，并不影响全球绝大多数地方的全天候、高精度、连续实时的导航定位测量。GPS 工作卫星的编号和试验卫星基本相同。

2. 地面监控系统

GPS 工作卫星的地面监控系统包括一个主控站、三个注入站和五个监测站。

对于导航定位来说 GPS 卫星是一个动态已知点。星的位置是依据卫星发射的星历——描述卫星运动及其轨道的参数算得的。每颗 GPS 卫星所播发的星历是由地面监控系统提供的。卫星上的各种设备是否正常工作以及卫星是否一直沿着预定轨道运行都要由地面设备进行监测和控制。地面监控系统另一重要作用是保持各颗卫星处于同一时间标准——GPS 时间系统。这就需要地面站监测各颗卫星的时间求出钟差，然后由地面注入站发给卫星，再由卫星将导航电文发给用户的 GPS 信号接收机。

3. GPS 信号接收机

GPS 信号接收机的任务是：能够捕获到按一定卫星高度截止角所选择的待测卫星的信号，并跟踪这些卫星的运行对所接收到的 GPS 信号进行变换、放大和处理，以便测量出 GPS 信号从卫星到接收机天线的传播时间，解译出 GPS 卫星所发送的导航电文，实时地计算出测站的三维位置甚至三维速度和时间。

GPS 卫星发送的导航定位信号是一种可供无数用户共享的信息资源。对于陆地、海洋和空间的广大用户，只要用户拥有能够接收、跟踪、变换和测量 GPS 信号的接收设备即 GPS 信号接收机，可以在任何时候用 GPS 信号进行导航定位测量。

根据使用目的的不同，用户要求的 GPS 信号接收机也各有差异。目前世界上已有几十家工厂生产 GPS 接收机，产品也有几百种。这些产品可以按照原理、用途、功能等来分类。

静态定位中 GPS 接收机在捕获和跟踪 GPS 卫星的过程中固定不变，接收机高精度地测量 GPS 信号的传播时间，利用 GPS 卫星在轨的已知位置解算出接收机天线所在位置的三维坐标。而动态定位则是用 GPS 接收机测定一个运动物体的运行轨迹。GPS 信号接收机所位于的运动物体叫做载体(如航行中的船舰、空中的飞机、行走的车辆等)。载体上的 GPS 接收机天线在跟踪 GPS 卫星的过程中相对地球而运动，接收机用 GPS 信号实时地测得运动载体的状态参数(瞬间三维位置和三维速度)。

接收机硬件和机内软件以及 GPS 数据的后处理软件包构成完整的 GPS 用户设备。GPS 接收机的结构分为天线单元和接收单元两大部分。对于测地型接收机来说，两个单元一般分成两个独立的部件，观测时将天线单元安置在测站上，接收单元置于观测站附近的适当地方，用电缆线将两者连接成一个整机。也有的 GPS 接收机将天线单元和接收单元制作成一个整体，观测时将其安置在观测站点上。

GPS 接收机一般用蓄电池作电源，同时采用机内机外两种直流电源。设置机内电池的目的是当更换机外电池时不会中断连续观测。在用机外电池的过程中，机内电池自动充电。关机后，机内电池为 RAM 存储器供电以防止丢失数据。

1.4.7 云计算技术

1. 云计算的概念与特点

云计算(cloud computing)是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法。过去往往用云来表示电信网，后来也用来表示互联网和底层基础设施。

云计算可以让使用者体验高达每秒 10 万亿次的运算能力，拥有这么强大的计算能力可以模拟核爆炸、预测气候变化和市场发展趋势。用户通过电脑、笔记本、手机等方式接入数据中心，按自己的需求进行运算。云计算系统的结构如图 1-7 所示。

云计算将计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，使企业数据中心的运行将与互联网更相似。这使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

正如从早期的单台发电机模式转向后来的电厂集中发电的模式，云计算意味着计算能力也可以作为一种商品进行流通，就像煤气、水电一样，使用方便，费用低廉。两者最大的不同在于，它的数据是通过互联网进行传输的。

云计算的主要特点如下：

1) 超大规模

“云”具有相当大的规模，Google 云计算已经拥有 100 多万台服务器，Amazon、IBM、微软、Yahoo 等的“云”均拥有几十万台服务器。企业私有云一般拥有数百上千台服务器。“云”能赋予用户前所未有的计算能力。

2) 虚拟化

云计算支持用户在任意位置、使用各种终端获取应用服务。所请求的资源来自“云”，而

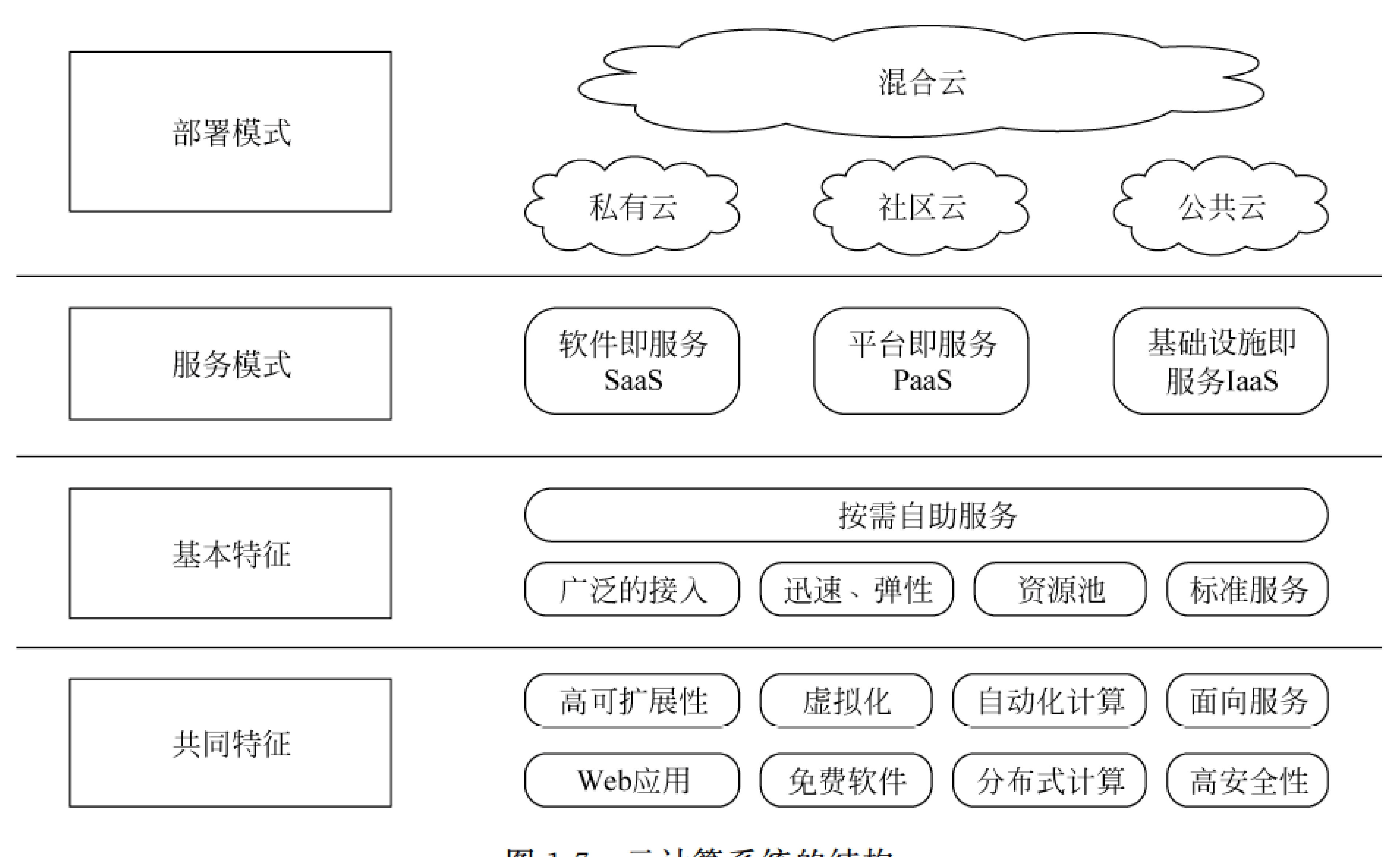


图 1-7 云计算系统的结构

不是固定的有形的实体。应用在“云”中某处运行，但实际上用户无须了解、也不用担心应用运行的具体位置。只需要一台笔记本或者一部手机，就可以通过网络服务来实现我们需要的一切，甚至包括超级计算这样的任务。

3）高可靠性

“云”使用了数据多副本容错、计算结点同构可互换等措施来保障服务的高可靠性，使用云计算比使用本地计算机可靠。

4）通用性

云计算不针对特定的应用，在“云”的支撑下可以构造出千变万化的应用，同一个“云”可以同时支撑不同的应用运行。

5）高可扩展性

“云”的规模可以动态伸缩，满足应用和用户规模增长的需要。

6）按需服务

“云”是一个庞大的资源池，让用户按需购买；云可以像自来水、电、煤气那样计费。

7）极其廉价

由于“云”的特殊容错措施可以采用极其廉价的结点来构成云，“云”的自动化集中式管理使大量企业无须负担日益高昂的数据中心管理成本，“云”的通用性使资源的利用率较之传统系统大幅提升，因此用户可以充分享受“云”的低成本优势，经常只要花费几百美元、几天时间，就能完成以前需要数万美元、数月时间才能完成的任务。

云计算可以彻底改变人们未来的生活，但同时也要重视环境问题，这样才能真正为人类进步做贡献，而不是简单的技术提升。

8）潜在的危险性

云计算服务除了提供计算服务外，还必然提供了存储服务。但是云计算服务当前垄断在私人机构（企业）手中，而他们仅仅能够提供商业信用。对于政府机构、商业机构（特别像

银行这样持有敏感数据的商业机构)对于选择云计算服务应保持足够的警惕。一旦商业用户大规模使用私人机构提供的云计算服务,无论其技术优势有多强,都不可避免地让这些私人机构以"数据(信息)"的重要性挟制整个社会。对于信息社会而言,"信息"是至关重要的。另一方面,云计算中的数据对于数据所有者以外的其他云计算用户是保密的,但是对于提供云计算的商业机构而言确实毫无秘密可言。所有这些潜在的危险,是商业机构和政府机构选择云计算服务、特别是国外机构提供的云计算服务时,不得不考虑的一个重要的因素。

2. 云计算的服务

云计算可以提供以下三个层次的服务:基础设施即服务(IaaS),平台即服务(PaaS)和软件即服务(SaaS)。

1) 基础设施即服务

基础设施即服务(Infrastructure-as-a-Service,IaaS),是指消费者通过 Internet 可以从完善的计算机基础设施获得服务。例如:硬件服务器租用。

2) 平台即服务

平台即服务(Platform-as-a-Service,PaaS)实际上是指将软件研发的平台作为一种服务,以 SaaS 的模式提交给用户。因此,PaaS 也是 SaaS 模式的一种应用。但是,PaaS 的出现可以加快 SaaS 的发展,尤其是加快 SaaS 应用的开发速度。例如:软件的个性化定制开发。

3) 软件即服务

软件即服务(Software-as-a-Service,SaaS)是一种通过 Internet 提供软件的模式,用户无须购买软件,而是向提供商租用基于 Web 的软件,来管理企业经营活动。例如:阳光云服务器。

1.4.8 数据挖掘技术

数据挖掘(Data Mining,DM),又翻译为资料探勘、数据采矿。它是数据库知识发现(Knowledge-Discovery in Databases,KDD)中的一个步骤。数据挖掘一般是指从大量的数据中通过算法搜索隐藏于其中信息的过程。数据挖掘通常与计算机科学有关,并通过统计、在线分析处理、情报检索、机器学习、专家系统(依靠过去的经验法则)和模式识别等诸多方法来实现上述目标。

数据挖掘是目前人工智能和数据库领域研究的热点问题,所谓数据挖掘是指从数据库的大量数据中揭示出隐含的、先前未知的并有潜在价值的信息的非平凡过程。数据挖掘是一种决策支持过程,它主要基于人工智能、机器学习、模式识别、统计学、数据库、可视化技术等,高度自动化地分析企业的数据,做出归纳性的推理,从中挖掘出潜在的模式,帮助决策者调整市场策略,减少风险,做出正确的决策。

数据挖掘的过程如图 1-8 所示。数据挖掘的过程由三个阶段组成:(1)数据准备;(2)数据挖掘;(3)结果评价与表达。数据挖掘可以与用户或知识库交互。

数据挖掘是通过分析每个数据,从大量数据中寻找其规律的技术,主要有数据准备、规律寻找和规律表示 3 个步骤。数据准备是从相关的数据源中选取所需的数据并整合成用于数据挖掘的数据集;规律寻找是用某种方法将数据集所含的规律找出来;规律表示是尽可

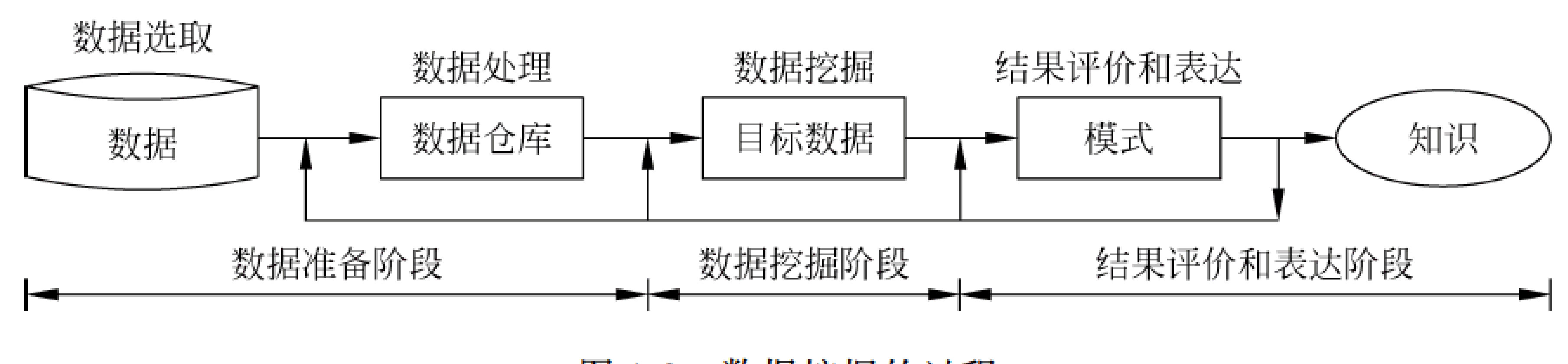


图 1-8　数据挖掘的过程

能以用户可理解的方式(如可视化)将找出的规律表示出来。

数据挖掘的任务有关联分析、聚类分析、分类分析、异常分析、特异群组分析和演变分析等。

从数据本身来考虑,通常数据挖掘需要有信息收集、数据集成、数据规约、数据清理、数据变换、数据挖掘实施过程、模式评估和知识表示 8 个步骤。

1. 信息收集

信息收集是根据确定的数据分析对象抽象出在数据分析中所需要的特征信息,然后选择合适的信息收集方法,将收集到的信息存入数据库。对于海量数据,选择一个合适的数据存储和管理的数据仓库是至关重要的。

2. 数据集成

数据集成是把不同来源、格式、特点性质的数据在逻辑上或物理上有机地集中,从而为企业提供全面的数据共享。

3. 数据规约

执行多数的数据挖掘算法即使在少量数据上也需要很长的时间,而做商业运营数据挖掘时往往数据量非常大。数据规约技术可以用来得到数据集的规约表示,它的数据量小得多,但仍然接近于保持原数据的完整性,并且规约后执行数据挖掘结果与规约前执行结果相同或几乎相同。

4. 数据清理

在数据库中的数据有一些是不完整的(有些感兴趣的属性缺少属性值),含噪声的(包含错误的属性值),并且是不一致的(同样的信息不同的表示方式),因此需要进行数据清理,将完整、正确、一致的数据信息存入数据仓库中,不然,挖掘的结果会差强人意。

5. 数据变换

数据变换通过平滑聚集、数据概化和规范化等方式,将数据转换成适用于数据挖掘的形式。对于某些实数型数据,通过概念分层和数据的离散化来转换数据也是关键的一步。

6. 数据挖掘过程

数据挖掘过程根据数据仓库中的数据信息,选择合适的分析工具,应用统计方法、事例

推理、决策树、规则推理、模糊集，甚至神经网络和遗传算法的方法处理信息，得出有用的分析信息。

7. 模式评估

模式评估是指从商业角度，由行业专家来分析、判断和验证数据挖掘结果的正确性。

8. 知识表示

知识表示将数据挖掘所得到的分析信息以可视化的方式呈现给用户，或作为新的知识存放在知识库中，供其他应用程序使用。

数据挖掘过程是一个反复循环的过程，每一个步骤如果没有达到预期目标，都需要回到前面的步骤，重新调整并执行。不是每项数据挖掘的工作都需要这里列出的每一步，例如在某项工作中不存在多个数据源的时候，步骤 2 数据集成的步骤便可以省略。

上述的步骤 3(数据规约)、步骤 4(数据清理)和步骤 5(数据变换)又统称为数据预处理阶段。在数据挖掘的过程中，至少 60%的成本要花在步骤 1 信息收集阶段，而至少 60%以上的精力和时间则是花在数据预处理阶段。

1.4.9 中间件技术

中间件(middleware)是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源。中间件位于客户机/服务器的操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口，但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递。通过中间件，应用程序可以工作于多种平台或操作系统(Operating System，OS)环境。

中间件是一类连接软件组件和应用的计算机软件，它包括一组服务。以便于运行在一台或多台机器上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进，该架构通常用于支持并简化那些复杂的分布式应用程序，它包括 Web 服务器、事务监控器和消息队列软件。

中间件是基础软件的一大类，属于可复用软件的范畴。顾名思义，中间件处于操作系统软件与用户的应用软件的中间。

中间件在操作系统、网络和数据库之上，应用软件的下层，总的作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活、高效地开发和集成复杂的应用软件。在众多关于中间件的定义中，被普遍接受的是国际数据公司(International Data Corporation，IDC)的表述：中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算资源和网络通信。

国际数据公司关于中间件的定义表明，中间件是一类软件，而非一种软件；中间件不仅仅实现互连，还要实现应用之间的互操作；中间件是基于分布式处理的软件，最突出的特点是其网络通信功能。

具体地说，中间件屏蔽了底层操作系统的复杂性，使程序开发人员面对一个简单而统一的开发环境，减少程序设计的复杂性，将注意力集中在自己的业务上，不必再为程序在不同

系统软件上的移植而重复工作，从而大大减少了技术上的负担。中间件带给应用系统的，不只是开发的简便、开发周期的缩短，也减少了系统的维护、运行和管理的工作量，还减少了计算机总体费用的投入。

由于标准接口对于可移植性、标准协议对于互操作性的重要性，中间件已成为许多标准化工作的主要部分。对于应用软件开发，中间件远比操作系统和网络服务更为重要，中间件提供的程序接口定义了一个相对稳定的高层应用环境，不管底层的计算机硬件和系统软件怎样更新换代，只要将中间件升级更新，并保持中间件对外的接口定义不变，应用软件几乎不需任何修改，从而保护了企业在应用软件开发和维护中的重大投资。

基于中间件的物联网终端体系结构如图 1-9 所示。

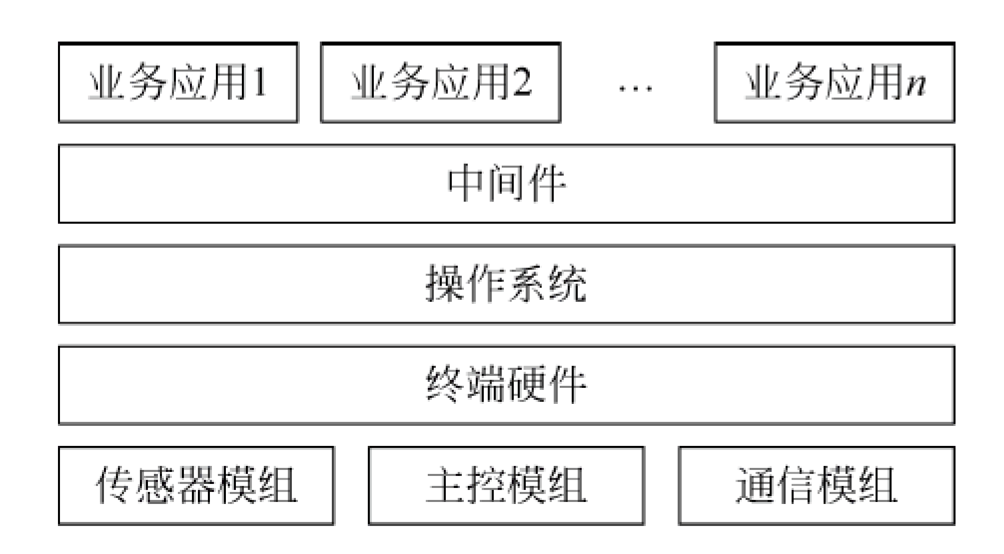


图 1-9　基于中间件的物联网终端体系结构

中间件大致可以分为六类：终端仿真/屏幕转换中间件、数据访问中间件、远程过程调用中间件、消息中间件、交易中间件、对象中间件。

物联网终端主要由传感器模组、主控模组和通信模组组成。中间件主要加载在主控模组上，这样可以加强终端管理功能。中间件对终端提供统一的接入规范，在通信层面屏蔽不同终端和外设传输协议的差异，实现标准化。

基于中间件技术开发的应用软件具有良好的可扩充性、易管理性、高可用性和可移植性。

1.5　物联网的标准体系

1.5.1　物联网标准体系的构建

物联网是跨行业、跨领域、具有明显交叉学科特征、面向应用的信息基础设施，因此构建物联网的标准体系时，不仅要考虑已有行业制订的标准，而且要兼顾物联网服务体系的发展需要；要避免不同行业标准组织的重复制订，还要做好各行业和部门间的协调合作，保证各自标准相互衔接，满足跨行业、跨地区的应用需求。物联网标准化体系应由物联网总体标准、物联网共性技术标准以及行业物联网标准构成。

物联网总体标准由基本类标准、物联网需求类标准、物联网架构类标准、物联网评估和测试类标准构成。

基本类标准将包括物联网基本术语、物联网的总体参考模型、物联网标准指南等；物联网需求类标准包括物联网的总体技术要求、物联网安全的总体技术要求、物联网服务质量总

体要求、物联网标识和解析总体需求；物联网架构类标准包括物联网系统的总体架构、物联网安全的总体架构、物联网标识和解析的总体架构、智慧城市总体架构等；物联网评估和测试类标准包括物联网应用评估、物联网公共测试等。

物联网共性技术标准包括信息感知技术类标准、信息传输技术类标准、信息开放技术类标准和信息处理技术类标准，这些标准是用于不同行业物联网的共性技术标准。物联网共性标准基于可重用于物联网应用的现有各类信息通信技术标准，同时各类 ICT 技术标准也面向物联网应用不断发展。

行业物联网标准由公共服务和智能电网、智能交通、智能医疗等垂直行业物联网标准构成。物联网的纵向模型分为感知层、网络层、应用层，因此行业物联网标准包括行业应用和公共服务特定的感知标准、网络标准和行业应用标准。行业物联网标准将遵循物联网总体性标准和共性技术标准的要求，面向行业应用需求，研制开发行业特有的技术、产品和应用类标准。

1.5.2 物联网标准化的特点

物联网不是全新的网络和应用。物联网是在现有电信网、互联网、行业专用网的基础上，增强网络延伸和信息感知的能力和信息处理能力，基于应用的需求构建的信息通信融合应用的基础设施，因此物联网不是新的网络和应用，而是多年来各行各业应用与信息通信技术融合发展的产物。

物联网的应用和感知设备呈现跨行业的多样性。物联网应用涉及经济与社会发展的各个行业和领域，并与各自业务流程紧密结合，具有应用跨度大、需求长尾化、产业分散度高、产业链长和技术集成性高的特点。物联网的应用按照最终用户来进行分类，可以分为公共服务(服务于普通消费者，例如智能家居、手机支付等)和行业服务(服务于各行各业，例如智能电网、智能物流等)。由于应用的不同，应用所需感知的内容不同，因此对感知设备的性能和接口要求也不一样。

物联网应用的服务对象包括各行各业，应用提供者利用信息通信技术和网络为其提供服务。物联网是各行各业应用与信息通信技术融合发展的产物，各行各业的应用提供者是物联网应用的主体，其应用种类繁多，需求差异较大。信息通信行业是其中一个行业，但因通信行业具有网络规模大、覆盖范围广的优势，因此能够为其他行业提供信息通信基础网络设施。

物联网的上述特点决定了物联网的标准化特点，即物联网的标准不是某一个行业或仅仅信息通信行业所能够单独完成的，而需要各行各业与信息通信行业共同制订，才能既符合行业需求，也能将最好的最适合的信息通信技术应用于各个行业，因此物联网的标准既包含行业应用和特定行业需求的标准，例如电力、交通、医疗等行业标准，同时也包含信息通信行业的标准，例如感知、通信和信息处理等技术标准。

1.5.3 物联网标准化的现状

基于以上的物联网标准化特点，物联网的标准化工作在全球的多个标准化组织竞相展开，包括国际标准化组织(如 ITU、ISO 和 IEC)、区域性标准化组织(如 ETSI)、国家标准化

组织(如 CCSA、ATIS、TTA、TTC)、行业标准化组织、论坛和任务组(如 IETF、IEEE、OMA)等,这些标准化组织各自沿着自己擅长的领域进行研究,所开发的标准有重叠也有分工,但他们之间的竞争大于合作,目前尚缺乏整体的协调、组织和配合。

在各标准化组织进行研究的同时,有些行业标准在国家或地区政府的推动下也在快速形成,这些行业应用的标准带动了相关标准化组织之间的分工和合作,为物联网标准做出了实质性的贡献。目前在行业应用标准化方面,智能电网、智能交通和智能医疗等方面的进展比较快。

1.5.4 物联网的国际标准

物联网涉及的范围很广,因此目前与之相关的国际标准化组织和工业标准化组织都在积极地从事物联网相关标准的研究和制订工作。以下介绍几个主要的标准化组织的研究进展情况。

国际电信联盟(ITU)提出的物联网体系架构如图 1-10 所示。

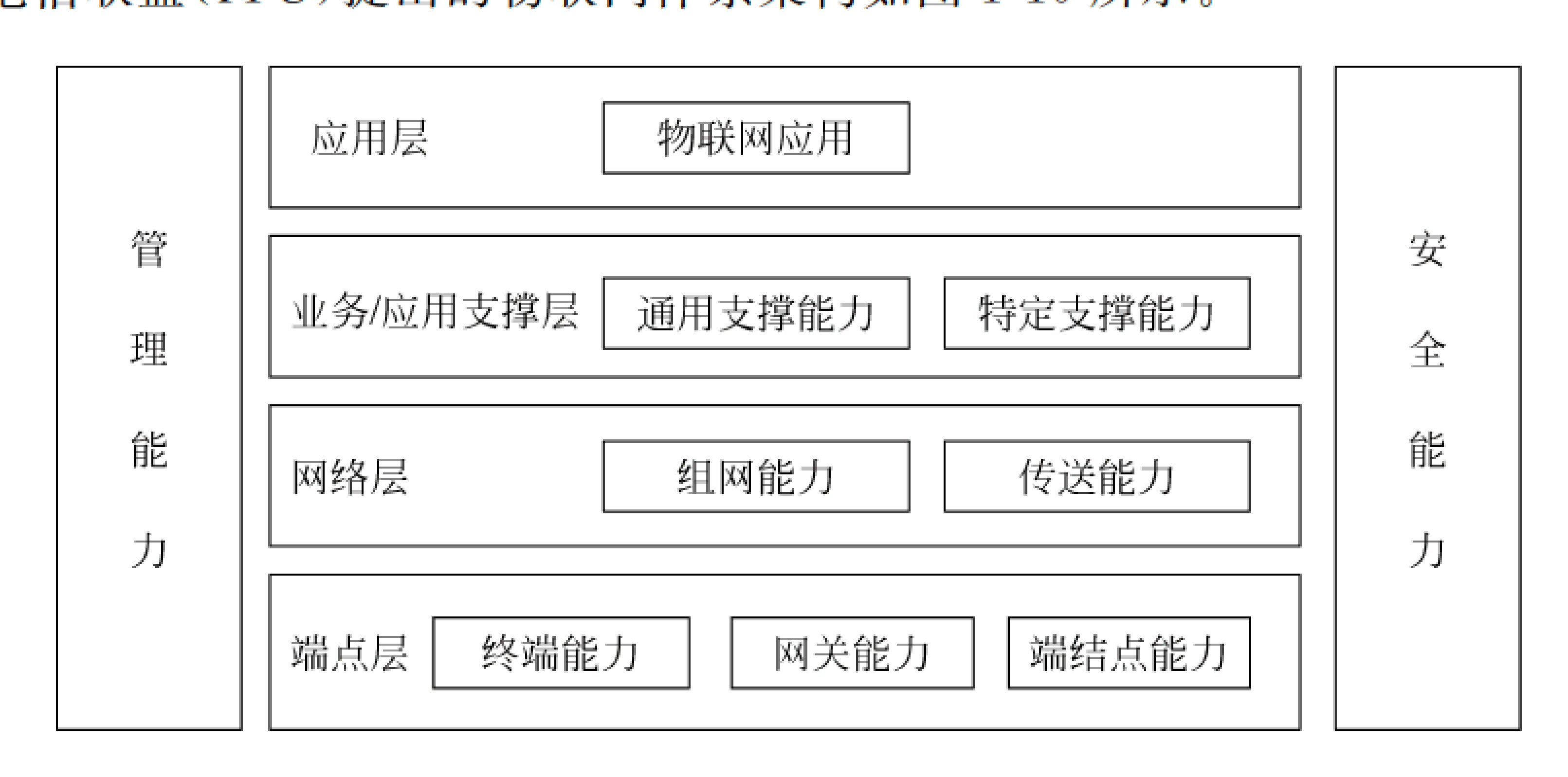


图 1-10 ITU 提出的物联网体系架构

国际电信联盟(International Telecommunication Union,ITU)专门成立了物联网全球标准化工作组(IoT-GSI),研究“物联网定义”和“物联网概述”两个国际标准,并在 2012 年 2 月份通过。

从图 1-10 中可以看出,在业务/应用支撑层能力、管理能力和安全能力方面都分为两个方面,即通用能力和面向某类应用的特定能力,比如智能电网和智能交通所需的能力可能不同。

电气和电子工程师协会(Institute of Electrical and Electronics Engineers,IEEE)主要研究 IEEE 802.15 低速近距离无线通信技术标准,并针对智能电网开展了大量工作。IEEE P2030 技术委员会成立于 2009 年 5 月,分为电力、信息和通信 3 个工作组,旨在为理解和定义智能电网互操作性提供技术基础和指南,针对 NIST 智能电网应用各个环节,帮助电力系统与应用和设备协同工作,确定模块和接口,为智能电网相关的标准制订奠定基础。IEEE 2010 年 4 月发布了 P2030 草案。

为了制订物联网标准,欧洲电信标准化协会(European Telecommunications Standards Institute,ETSI)也成立了 M2M 技术委员会,对 M2M 需求、网络架构、智能电网、智能医疗、城市自动化等方面进行了研究,并陆续出台了多个技术规范。

互联网工程任务组(Internet Engineering Task Force,IETF)则制订了以 IP 协议为基础的,适应感知延伸层特点的组网协议。目前 IETF 的工作主要集中于 6LoWPAN 和 ROLL 协议两个方面,6LoWPAN 以 IEEE 802.15.4 为基础,针对传感器结点低开销、低复杂度、低功耗的要求,对现有 IPv6 系统进行改造,压缩包头信息,提高对感知延伸层应用的使用能力。而 ROLL 的目标是使公共的、可互操作的第 3 层路由能够穿越任何数量的基本链路层协议和物理媒体。例如,一个公共路由协议能够工作在各种网络,如 802.15.4 无线传感网络、蓝牙个人区域网络以及未来低功耗 802.11Wi-Fi 网络之内和之间。

目前,6LoWPAN 已进入标准化的中期阶段,而 ROLL 仍处于草案阶段。

第三代合作伙伴计划(3rd Generation Partnership Project,3GPP)是 3G 技术标准的制订机构,由欧洲的 ETSI、日本的 ARIB 和 TTC、韩国的 TTA 和美国的 T1 在 1998 年底发起并成立,目标旨在研究制订并推广基于演进的 GSM 核心网络的 3G 标准,即 WCDMA、TD-SCDMA、EDGE 等。中国无线通信标准组(CWTS)于 1999 年加入 3GPP。

3GPP 结合移动通信网研究 M2M 的需求、架构以及对无线接入的优化技术;其 SA 和 RAN 分别针对网络架构、核心网以及无线接入网开展了工作,目前网络架构的增强已经进入实质性工作阶段,而无线接入网的增强仍处于研究阶段。

ZigBee 联盟的 ZigBee 协议基于 IEEE 802.15.4 的物理层和媒体访问控制(MAC)层技术,重点制订了网络层和应用层协议,支持 Mesh 和簇状动态路由网络,在目前的无线传感器网络中得到广泛应用。

1.5.5 物联网的中国标准

中国通信标准化协会(CCSA)于 2010 年 2 月专门成立了“泛在网技术工作委员会”(TC10),下设 4 个工作组,对物联网的共性总体标准、应用标准、网络标准和感知延伸等标准进行了全面的研究和行业标准的制订。

自成立以来,TC10 已共计完成行标、技术报告和研究课题立项 31 项,内容涵盖了物联网标准体系中的 3 个层次以及相关的总体架构和公共技术。其中,涉及总体架构和公共技术的立项 6 项,涉及物联网应用层的立项 16 项,涉及物联网网络层的立项 4 项,涉及物联网感知延伸层的立项 5 项。同时 CCSA 与智能交通标准工作组签订了合作协议,对智能交通的标准进行合作。

1.6 物联网的典型应用

毫无疑问,“物联网”时代的来临,一定会给我们的工作和生活带来翻天覆地的变化。物联网技术的用途广泛,遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、环境监测、路灯照明管控、景观照明管控、楼宇照明管控、广场照明管控、老人护理、个人健康、花卉栽培、水系监测、食品溯源、敌情侦查和情报搜集等多个领域。

物联网把新一代的信息技术充分运用在各行各业之中,具体地说,就是把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等各种物体中,然后将“物联网”与现有的互联网整合起来,实现人类社会与物理系统的整合,在这个整合的网络当

中，存在能力超级强大的中心计算机群，能够对整合网络内的人员、机器、设备和基础设施实施实时的管理和控制，在此基础上，人类可以以更加精细和动态的方式管理生产和生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然间的关系。

1.6.1 物联网在家庭中的应用

应用物联网技术的智能家居系统，依照人体工程学原理，融合个性需求，将与家居生活有关的各个子系统，如安防、照明控制、窗帘控制、煤气阀控制、多媒体、家用电器、地板采暖等有机地结合在一起，通过网络化综合智能控制和管理，实现“以人为本”的全新家居生活体验。

假如拥有了智能家居系统，当你不在家时，你可以远程监视家中的孩子或老人的状况；你可以在回到家之前打开家里空调；当你回到家时，你家的大门会自动为你打开；空调已经在工作，吹出令人舒适的凉风，而原来处于通风状态而打开的门窗也随着空调的启动而自动关闭，使室内气温刚好达到了适合人体的温度；当你进入家门后，只要按一下“回家”键，家中的电视自动开启，室内灯光自动点亮，背景音乐自动响起；你的冰箱会将你最需要的食物下单通知商家，为你配送到家；当你家中的甲醛、一氧化碳、二氧化碳等有毒有害气体超标时，新鲜空气系统会自动启动，主人的手机也会接到报警短信提醒；你只要用一个遥控器就能控制家中所有的电器；当你要外出时，只要按一下“离家”键，家中所有需要关闭的灯和电器自动关闭，安防系统会自动开启；当你家中没人时，园艺系统自动为你洒水、施肥、喷药；当你家中的电器出现了故障，物联网也能自动感知并提醒主人维修公司的联系方式，帮助你预约维修人员上门修理……

1.6.2 物联网在医学中的应用

医学物联网，就是将物联网技术应用于医疗、健康管理、老年健康照顾等医学领域。

医学物联网中的“物”，就是各种与医疗服务活动相关的人和事物，如健康者、亚健康者、病人、医生、护士、医疗设备、身体检测仪器、药品等。医学物联网中的“联”，即信息交互连接，把上述“事物”产生的相关信息交互、传输和共享。医学物联网中的“网”是通过把“物”有机地连成一张“网”，就可感知医学服务对象、各种数据的交换和无缝连接，达到对医疗卫生保健服务的实时动态监控、连续跟踪管理和精准的医疗健康决策。

那么什么是“感”、“知”、“行”呢？“感”就是数据采集和信息获得，例如，连续监测患者的体温、血压、脉搏等人体特征参数、周边环境信息、感知设备和人员情况等。“知”特指数据分析，如高血压患者连续的血压值测到之后，计算机会自动分析出他的血压状况是否正常，如果不正常，就会生成警报信号，及时通知医生知晓情况，调整医疗方案，并加以实施，这就是“行”。

应用物联网技术的智慧健康，将数字健康档案、动态健康管理、医疗服务平台三者的有机结合，通过自我健康管理(健康教育、健康记录等)、健康监测(包括智能健康指标检测、健康预警、健康指导等)、远程医疗协助(包括用药指导、膳食指导、运动指导、慢性康复指导等)，相互作用，环环相扣，实现对个体健康的全程智能管理。

你如果拥有了智慧健康系统，你可以随时用电子秤、人体脂肪分析仪、电子体温计、血压计和心率监测仪等人体状况传感设备，自动测量自己的血压、血糖、血氧、心电等与健康有关

的数据，管理自己的健康记录；你也可以选择让你的健康数据自动传送到健康控制中心，你的健身教练将根据健康数据帮助你制订下一步的健身计划和健康食谱，你的特约医生将根据健康数据了解你的健康状况，必要时可以对你进行远程会诊，再提出医疗意见；家有老人如果突发疾病，信息会自动发送给子女，并会自动传送医院的急救中心……

1.6.3 物联网在交通中的应用

应用物联网技术的智能交通系统，利用交通信息系统、交通监控系统、旅行信息系统、智能旅游系统、车载智能信息设备等，提供实时的交通路况和停车信息，进行智能的分析、控制与引导，提高出行者的方便感和舒适度。

你如果拥有了智能交通系统，当你开车出门时，智能手机和车载智能导航仪能显示实时路况、自动帮你选择最近或最快路径；你要停车，可以查到附近停车场的位置和路径，现在还剩下多少车位、你进入该停车场时还有空车位的概率是多少等信息，你还可以预定车位；你停车时万一忘了锁车门，你离开 20 米以外的时间超过 30 秒，车子将会自动把车门锁好，当有人动你的车子，你的手机会收到报警信号；当你在半路上想就餐，只要打开手机，输入“饭店”，搜索引擎就把你所在位置附近的餐厅的地图呈现在你的手机屏幕上；当你到某个风景区旅游，智能导游仪可以图文并茂地为你讲解每个景点的详细情况……

安全是交通管理的最重要的一环。对于智能交通规划和管理来说，交通安全也是在规划中不可或缺的部分。要保障交通安全，需要各种各样的手段进行综合配套管理，包括对酒驾行为的严厉打击、交通设施的完善、交通行为的规范等。

疲劳驾驶是交通事故、交通意外的最重要的诱因之一，所以对于疲劳驾驶的预防和管理都一直受到高度的重视。早期的措施一般是从管理制度上去要求，如持续行驶高速 4 小时需要进入服务站休息、更换司机等。现在随着物联网感知技术的发展，基于智能视频分析的疲劳检测技术也开始进入实用阶段。

基于智能视频分析的疲劳检测技术，是通过对人眼、面部细微特征进行分析，并结合车辆行驶速度等要素，对处于疲劳状态的驾驶员实现本地的声光提醒，使驾驶员一直处于良好的精神状态，防止安全事故的发生。通过智能视频分析技术，普通视频采集设备将变身为智能物联网感知器，可以感知很多关键信息。

在智能交通系统中，通过对客流统计数据、违规车牌照片、司机疲劳状态等关键信息的再利用，为智能交通中的交通调度、交通规划、交通行为管理以及交通安全预防都可以提供非常优秀的应用。

1.6.4 物联网在物流中的应用

美国 IBM 公司于 2009 年提出了“智慧供应链”的概念，即建立一个面向未来的具有先进、互联和智能三大特征的供应链，通过传感器、RFID 标签、制动器、GPS 和其他设备及系统产生实时的物流信息，紧接着“智慧物流”的概念由此延伸而出。

与智能物流强调构建一个虚拟的物流动态信息化的互联网管理体系不同，“智慧物流”更重视将物联网、传感网与现有的互联网整合起来，通过精细、动态、科学的管理，实现物流的自动化、可视化、可控化、智能化、网络化，从而提高资源利用率和生产力水平，创造更丰富

社会价值的综合内涵。

在2009年，美国总统奥巴马提出将“智慧的地球”作为美国国家战略，认为IT产业下一阶段的任务是把新一代IT技术充分运用到各行各业之中，具体地说，就是把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等各种物体中，并且被普遍连接，形成所谓“物联网”，然后将“物联网”与现有的互联网整合起来，实现人类社会与物理系统的整合，在这个整合的网络当中，存在能力超级强大的中心计算机群，能够对整合网络内的人员、机器、设备和基础设施实施实时的管理和控制，在此基础上，人类可以以更加精细和动态的方式管理生产和生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然间的关系。

智慧物流是利用集成智能化技术，使物流系统能模仿人的智能，具有思维、感知、学习、推理判断和自行解决物流中某些问题的能力。即在流通过程中获取信息从而分析信息做出决策，使商品从源头开始被实施跟踪与管理，实现信息流快于实物流。即可通过RFID、传感器、移动通信技术等让配送货物自动化、信息化和网络化。

国际电信联盟于2005年的报告曾描绘“物联网”时代的图景：当司机出现操作失误时汽车会自动报警；公文包会提醒主人忘带了什么东西；衣服会“告诉”洗衣机对颜色和水温的要求等。物联网在物流领域内的典型应用情景是：假如物流公司的某辆货车应用了物联网技术，那么当装载超重时，汽车会自动告诉司机超载了，并且超载多少，但空间还有剩余，还会建议司机轻重货物应该如何搭配；当搬运人员野蛮卸货时，某件货物可能会大叫：“你扔疼我了”，或者说“亲爱的，请你不要太粗鲁，可以吗?”；当司机在和别人扯闲话，货车会模仿老板的声音大喊：“帅哥，该发车了!”

1.6.5　物联网在安防中的应用

物联网技术的普及应用，使得城市的安防从过去简单的安全防护系统向城市综合化体系演变，城市的安防项目涵盖众多的领域，有街道社区、楼宇建筑、银行邮局、道路监控、机动车辆、警务人员、移动物体、船只等。特别是针对重要场所，例如，机场、码头、水电气厂、桥梁大坝、河道、地铁等场所，引入物联网技术后可以通过无线移动、跟踪定位等手段建立全方位的立体防护。

物联网安防兼顾了整体城市管理系统、环保监测系统、交通管理系统、应急指挥系统等应用的综合体系。特别是车联网的兴起，在公共交通管理上、车辆事故处理上、车辆偷盗防范上可以更加快捷准确的跟踪定位处理。还可以随时随地的通过车辆获取更加精准的灾难事故信息、道路流量信息、车辆位置信息、公共设施安全信息、气象信息等等信息来源。

智能化安防技术的主要内涵是其相关内容和服务的信息化、图像的传输和存储、数据的存储和处理等。

从产品的角度上分析：智能化安防系统应具备防盗报警系统、视频监控报警系统、出入口控制报警系统、保安人员巡更报警系统、GPS车辆报警管理系统和110报警联网传输系统等子系统。这些子系统可以是单独设置、独立运行，也可以由中央控制室集中进行监控，还可以与其他综合系统进行集成和集中监控。

防盗报警系统分为边界防卫、建筑物区域内防卫、单位企业空旷区域内防卫、单位企业内实物设备器材防卫等。系统的前端设备为各种类别的报警传感器或探测器；系统的终端

是显示/控制/通信设备，它可应用独立的报警控制器，也可采用报警中心控制台控制。不论采用什么方式控制，均必须对设防区域的非法入侵进行实时、可靠和正确无误的复核和报警。漏报警是绝对不允许发生的，误报警应该降低到可以接受的限度。考虑到值勤人员容易受到作案者的武力威胁与抢劫，系统应设置紧急报警按钮，并留有与110报警中心联网的接口。

视频监控报警系统常规应用于建筑物内的主要公共场所和重要部位进行实时监控、录像和报警时的图像复核。视频监控报警系统的前端是各种摄像机、视频检测报警器和相关附属设备；系统的终端设备是显示/记录/控制设备，常规采用独立的视频监控中心控制台或监控报警中心控制台。安全防范用的视频监控报警系统常规应与防盗报警系统、出入口控制系统联动，由中央控制室进行集中管理和监控。独立运行的视频监控报警系统，画面显示能任意编程、自动或手动切换，画面上必须具备摄像机的编号、地址、时间、日期等信息显示，并能自动将现场画面切换到指定的监视器上显示，对重要的监控画面应能长时间录像。这类系统应具备紧急报警按钮和留有110报警中心联网的通信接口。

出入口控制报警系统是采用现代电子信息技术，在建筑物的出入口对人(或物)的进出，实施放行、拒绝、记录和报警等操作的一种自动化系统。这种操作系统通常由出入口目标识别系统、出入口信息管理系统、出入口控制执行机构三个部分组成。系统的前端设备为各类出入口目标识别装置和门锁开启闭合执行机构；传输方式采用专线或网络传输；系统的终端设备是显示/控制/通信设备，常规采用独立的门禁控制器，也可通过计算机网络对各门禁控制器实施集中监控。出入口控制报警系统常规要与防盗报警系统、闭路视频监控报警系统和消防系统联动，才能有效地实现安全防范。出入口目标识别系统可分为对人的识别和对物的识别。以对人的识别为例，可分为生物特征系统和编码标识别系统两类。

一个完整的智能化视频监控安全防范系统，还应包括安保人员巡更报警系统，访客报警系统以及其他智能化安全防范系统。巡更报警系统通过预先编制的保安巡逻软件，应用通行卡读出器对保安人员巡逻的运动状态(是否准时，遵守顺序等)进行监督，作出记录，并对意外情况及时报警。访客报警系统是使居住在大楼内的人员与访客能双向通话或可视通话，大楼内居住的人员可对大楼内的入口门或单元门实施遥控开启或关闭，当发生意外情况时能及时向保安中心报警。

其他智能化安全防范系统是根据特殊的安全防范管理工作的需要而设置的。如GPS车辆报警管理系统和110报警联网传输系统，还必须对车库(或停车场等)内车辆通行道路口实施出入控制、监视、行车信号指示以及停车计费等综合管理；另外如重要仓库的安全防范系统，必须对建筑物内的重要仓储库，进行有效的出入口控制、防盗、监视控制和管理等。

1.6.6 物联网在电网中的应用

智能电网又称为“电网2.0”，就是将物联网技术应用到电力网络中，实现电网管理的智能化。

智能电网建立在集成的、高速的、双向的通信网络基础上，通过先进的传感和测量技术、先进的设备技术、先进的控制方法以及先进的决策支持系统技术的应用，实现电网的可靠、安全、经济、高效、环境友好和使用安全的目标，其主要特征包括自愈、激励用户、抵御攻击、提供满足用户需求的电能质量、容许各种不同发电形式的接入、启动电力市场以及资源的优

化高效运行。

智能电网由很多部分组成，可分为：智能变电站、智能配电网、智能电能表、智能交互终端、智能调度、智能家居、智能用电楼宇、智能城市用电网、智能发电系统、新型储能系统等。

建立高速、双向、实时、集成的通信系统是实现智能电网的基础，没有这样的通信系统，任何智能电网的特征都无法实现，因为智能电网的数据获取、保护和控制都需要这样的通信系统的支持，因此建立这样的通信系统是迈向智能电网的第一步。同时通信系统要和电网一样深入到千家万户，这样就形成了两张紧密联系的网络，即电网和通信网络，只有这样才能实现智能电网的目标和主要特征。

参数量测技术是智能电网基本的组成部件，先进的参数量测技术获得数据并将其转换成数据信息，以供智能电网的各个方面使用。它们评估电网设备的健康状况和电网的完整性，进行表计的读取、消除电费估计以及防止窃电、缓减电网阻塞以及与用户的沟通。

未来的智能电网将取消所有的电磁表计及其读取系统，取而代之的是可以使电力公司与用户进行双向通信的智能固态表计。基于微处理器的智能表计将有更多的功能，除了可以计量每天不同时段电力的使用和电费外，还有存储电力公司下达的高峰电力价格信号及电费费率，并通知用户实施什么样的费率政策。更高级的功能有用户自行根据费率政策，编制时间表，自动控制用户内部电力使用的策略。

智能电网广泛应用先进的设备技术，极大地提高输配电系统的性能。未来的智能电网中的设备将充分应用在材料、超导、储能、电力电子和微电子技术方面的最新研究成果，从而提高功率密度、供电可靠性和电能质量以及电力生产的效率。

未来智能电网将主要应用三个方面的先进技术：电力电子技术、超导技术以及大容量储能技术。通过采用新技术和在电网和负荷特性之间寻求最佳的平衡点来提高电能质量。通过应用和改造各种各样的先进设备，如基于电力电子技术和新型导体技术的设备，来提高电网输送容量和可靠性。配电系统中要引进许多新的储能设备和电源，同时要利用新的网络结构，如微电网。

先进的控制技术是指智能电网中分析、诊断和预测状态并确定和采取适当的措施以消除、减轻和防止供电中断和电能质量扰动的装置和算法。这些技术将提供对输电、配电和用户侧的控制方法并且可以管理整个电网的有功和无功。从某种程度上说，先进控制技术紧密依靠并服务于其他四个关键技术领域，如先进控制技术监测基本的元件（参数量测技术），提供及时和适当的响应（集成通信技术；先进设备技术）并且对任何事件进行快速的诊断（先进决策技术）。另外，先进控制技术支持市场报价技术以提高电力资产的管理水平。

未来先进控制技术的分析和诊断功能将引进预设的专家系统，在专家系统允许的范围内，采取自动的控制行动。这样所执行的行动将在秒一级水平上，这一自愈电网的特性将极大地提高电网的可靠性。当然先进控制技术需要一个集成的高速通信系统以及对应的通信标准，以处理大量的数据。先进控制技术将支持分布式智能代理软件、分析工具以及其他应用软件。

决策支持技术将复杂的电力系统数据转化为系统运行人员一目了然的可理解的信息，运用动画技术、动态着色技术、虚拟现实技术以及其他数据展示技术来帮助系统运行人员认识、分析和处理紧急问题。

在许多情况下，系统运行人员做出决策的时间从小时缩短到分钟，甚至到秒，这样智能

电网需要一个广阔的、无缝的、实时的应用系统、工具和培训，以使电网运行人员和管理者能够快速的做出决策。

1.7 本章小结

物联网是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备，按照约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

物联网具备四个特征：全面感知、可靠传输、智能处理和综合应用。

物联网体系结构分为三个层次：感知层、网络层、应用层。

感知层由传感器结点和接入网关等组成，传感器感知外部世界的温度、湿度、声音和图像等信息，并传送到上层的网关，由网关将收集到的信息通过网络层提交到后台处理。当后台对数据处理完毕后，发送执行命令到相应的执行机构，完成对被控对象或被测对象的控制参数调整，或者发出某种信号以实现远程监控。

网络层是物联网的神经中枢和大脑。实现信息传递和处理。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等。网络层将感知层获取的信息进行传递和处理，类似于人体结构中的神经中枢和大脑。

应用层主要是根据行业特点，借助物联网的技术手段，开发各类的行业应用解决方案，将物联网的优势与行业的生产经营、信息化管理、组织调度结合起来，形成各类的物联网解决方案，构建智能化的行业应用。

物联网的关键技术很多，主要包括 RFID 技术、无线传感器网络技术、M2M 技术、GPS 全球定位技术、云计算技术、数据挖掘技术、中间件技术、IPv6 技术等。

RFID 是一种无线通信技术，可以通过无线电讯号识别特定目标并读写相关数据，而无须识别系统与特定目标之间建立机械或者光学接触。

无线传感器网络(Wireless Sensor Network，WSN)是由大量的静止或移动的传感器以自组织和多跳的方式构成的无线网络，以协作地感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给网络的所有者。

M2M 是“机器对机器通信(Machine to Machine)”或者“人对机器通信(Man to Machine)”的简称，主要是指通过“通信网络”传递信息从而实现机器对机器或人对机器的数据交换，也就是通过通信网络实现机器之间或人与机器之间的互联、互通。

GPS 全球定位系统是由空间星座、地面控制和用户设备三部分构成的。GPS 技术能够快速、高效、准确地提供点、线、面要素的精确三维坐标以及其他相关信息，具有全天候、高精度、自动化、高效益等显著特点，广泛应用于军事、民用交通(船舶、飞机、汽车等)导航、大地测量、摄影测量、野外考察探险、土地利用调查、精确农业以及日常生活(人员跟踪、休闲娱乐)等不同领域。

云计算(cloud computing)是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法。过去往往用云来表示电信网，后来也用来表示互联网和底层基础设施的抽象。

数据挖掘一般是指从大量的数据中通过算法搜索隐藏于其中信息的过程。数据挖掘通

常与计算机科学有关，并通过统计、在线分析处理、情报检索、机器学习、专家系统(依靠过去的经验法则)和模式识别等诸多方法来实现上述目标。

中间件(middleware)是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源。中间件位于客户机/服务器的操作系统之上，管理计算机资源和网络通信，是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口，但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递。通过中间件，应用程序可以工作于多平台或操作系统(Operating System，OS)环境。

IPv6是英文Internet Protocol Version 6的缩写，其中Internet Protocol译为"互联网协议"。IPv6是互联网工程任务组(Internet Engineering Task Force，IETF)设计的用于替代现行版本IP协议(IPv4)的下一代IP协议。IPv6这不但解决了网络地址资源数量的问题，同时也为除电脑以外的海量传感器连入物联网在数量限制上扫清了障碍。

目前，物联网的标准化工作在全球的多个标准化组织竞相展开，包括国际标准化组织(如ITU、ISO和IEC)、区域性标准化组织(如ETSI)、国家标准化组织(如CCSA、ATIS、TTA、TTC)、行业标准化组织、论坛和任务组(如IETF、IEEE、OMA)等，这些标准化组织各自沿着自己擅长的领域进行研究，所开发的标准有重叠也有分工，但他们之间的竞争大于合作，尚缺乏整体的协调、组织和配合。

物联网的用途广泛，遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监测、环境监测、路灯照明管控、景观照明管控、楼宇照明管控、广场照明管控、老人护理、个人健康、花卉栽培、水系监测、食品溯源、敌情侦查和情报搜集等多个领域。

在本章的最后，还简要地介绍了物联网在家庭、医学、交通、物流、安防、电网等方面的典型应用。

应用物联网技术的智能家居，依照人体工程学原理，融合个性需求，将与家居生活有关的各个子系统如安防、照明控制、窗帘控制、煤气阀控制、多媒体、家用电器、地板采暖等有机地结合在一起，通过网络化综合智能控制和管理，实现"以人为本"的全新家居生活体验。

医学物联网中的"物"，就是各种与医疗服务活动相关的人和事物，如健康者、亚健康者、病人、医生、护士、医疗设备、身体检测仪器、药品等。医学物联网中的"联"，即信息交互连接，把上述"事物"产生的相关信息交互、传输和共享。医学物联网中的"网"是通过把"物"有机地连成一张"网"，就可感知医学服务对象、各种数据的交换和无缝连接，达到对医疗卫生保健服务的实时动态监控、连续跟踪管理和精准的医疗健康决策。

应用物联网技术的智能交通系统，利用交通信息系统、交通监控系统、旅行信息系统、智能旅游系统、车载智能信息设备等，提供实时的交通路况和停车信息，进行智能的分析、控制与引导，提高出行者的方便和舒适度。

智慧物流是利用集成智能化技术，使物流系统能模仿人的智能，具有思维、感知、学习、推理判断和自行解决物流中某些问题的能力。即在流通过程中获取信息从而分析信息做出决策，使商品从源头开始被实施跟踪与管理，实现信息流快于实物流。即可通过RFID、传感器、移动通信技术等让配送货物自动化、信息化和网络化。

物联网技术的普及应用，使得城市的安防从过去简单的安全防护系统向城市综合化体系演变，城市的安防项目涵盖众多的领域，有街道社区、楼宇建筑、银行邮局、道路监控、机动车辆、警务人员、移动物体、船只等。特别是针对重要场所，例如：机场、码头、水电气厂、桥

梁大坝、河道、地铁等场所，引入物联网技术后可以通过无线移动、跟踪定位等手段建立全方位的立体防护。

智能电网建立在集成的、高速的、双向的通信网络基础上，通过先进的传感和测量技术、先进的设备技术、先进的控制方法以及先进的决策支持系统技术的应用，实现电网的可靠、安全、经济、高效、环境友好和使用安全的目标，其主要特征包括自愈、激励用户、抵御攻击、提供满足用户需求的电能质量、容许各种不同发电形式的接入、启动电力市场以及资源的优化高效运行。

复习思考题

1. 请简述物联网的起源和发展。
2. 请简述物联网的定义。
3. 请指出物联网的四个特征。
4. 请画图表示物联网的体系结构，并分别说明每一层实现的功能。
5. 什么是 RFID 技术?
6. 什么是无线传感器网络技术?
7. 什么是 M2M 技术?
8. 什么是 Wi-Fi 技术?
9. 什么是 WiMAX 技术?
10. 什么是 ZigBee 技术?
11. 什么是蓝牙技术?
12. 什么是 GPS 全球定位技术?
13. 什么是云计算技术? 云计算的主要特点是什么?
14. 什么是数据挖掘技术?
15. 什么是中间件技术?
16. 什么是 IPv6 技术?
17. 物联网的总体标准主要包括哪些组成部分?
18. 请简要介绍物联网的国际标准。
19. 请简要介绍物联网的中国标准。
20. 请说明物联网在家庭方面的典型应用。
21. 请说明物联网在医学方面的典型应用。
22. 请说明物联网在交通方面的典型应用。
23. 请说明物联网在物流方面的典型应用。
24. 请说明物联网在安防方面的典型应用。
25. 请说明物联网在电网方面的典型应用。

第2章 物联网安全概述

2.1 物联网的安全特征

物联网安全是指物联网系统可以连续地、可靠地和正常地运行，服务不会中断，物联网系统中的软件、硬件和系统中的数据受到保护，不受人为的恶意攻击、破坏和更改。

感知信息的多样性、网络环境的复杂性和应用需求的多样性，使物联网安全面临新的严峻的考验。信息和网络安全的目标是保证被保护信息的机密性、完整性和可利用性。物联网以数据为中心并且与应用密切相关，这一特征决定了物联网总体安全目标要达到机密性，避免攻击者读取机密信息；物联网系统应具有数据鉴别能力，避免结点被注入虚假信息；物联网系统应具有设备鉴别能力，避免非法设备接入物联网；物联网系统应保证数据完整性，校验数据是否被修改；物联网系统还应具有可用性，保证系统的网络服务无论在任何时间都可以提供给合法的用户。

2.1.1 传统网络面临的安全威胁

物联网是基于互联网技术将设备连接起来的一个综合性网络，因此，互联网技术是物联网的基础，互联网的安全直接关系到整个物联网的安全。互联网安全问题涉及网络设备基础安全、网络安全、Web 安全和基于 Web 应用的安全等各个方面，包括安全编码、数据帧安全和密钥管理与交换等。

1. 安全编码

由于任意一个标签的标识或识别码都能被远程主机任意地扫描，标签可能会自动地、不加区分地回复读写器的指令，并且将其所存储的信息传输给读写器，因此编码的安全性必须引起重视。

2. 数据帧安全

由于在互联网信息传输环境中，攻击者可能会窃听和截取数据帧的内容，获取相关的信息，并为进一步攻击做准备，因此，必须重视数据帧的安全。

3. 密钥管理与交换

在互联网中实施的机密性和完整性措施，关键在于密钥的建立和管理过程，由于物联网

中结点的计算能力和电源供给能力等都有限,因此传统的密钥管理方式不适用于物联网。

2.1.2 物联网面临的安全威胁

根据物联网本身的特点,物联网除了面临传统网络的安全问题以外,还存在一些与现有的互联网安全不一样的特殊安全问题。这是因为物联网是由大量的传感器等设备构成的,缺少人对设备的有效监控,并且物联网设备种类繁多、数量庞大,所以物联网还面临其特有的安全威胁。

1. 点到点消息认证

由于物联网的应用可以取代人来完成一些复杂、危险和机械的工作,物联网传感器和设备往往部署在无人监控的场景中,因此攻击者可以轻易接近这些设备,从而对它们进行破坏,甚至通过本地操作更换机器的软硬件,使得物联网中有可能存在大量的恶意结点和已经损坏的结点。

2. 重放攻击

在物联网的标签体系中,如果系统无法区分信息是否曾经传递给读写器,攻击者可以冒充合法者的身份,重放截获信息,从而获得相应的服务。

3. 拒绝服务攻击

一方面物联网以域名服务(Domain Name Service,DNS)技术为基础,同样也继承了DNS技术的安全隐患;另一方面由于物联网中结点数量庞大、且以集群方式布置,因此在传输数据时,由于大量机器的数据发送会引起网络拥塞,形成拒绝服务攻击。另外,攻击者广播Hello信息,或者利用通信机制中的优先级策略、虚假路由等协议的安全漏洞,同样可以发起拒绝服务攻击。

4. 篡改或泄漏标签数据

攻击者一方面可以破坏标签数据,使得物品服务不可正常使用;另一方面可能会窃取标签数据,获得相关的服务,为进一步攻击做准备。

5. 权限提升攻击

攻击者通过协议漏洞或物联网的其他脆弱环节,使得物品服务获得高级别服务,甚至可以控制物联网其他结点的运行。

6. 业务安全

传统的认证是区分不同层次的,例如网络层的认证负责网络层的身份鉴别,业务层的认证负责业务层的身份鉴别,两者独立存在。然而在物联网体系中,在多数的情况下,设备都有专门的用途,其业务应用与网络通信紧密地捆绑在一起。由于网络层的认证是必不可少的,因此业务层的认证机制就不再是必需的,而是根据业务由谁来提供和业务的敏感程序来设计。

7. 隐私安全

在物联网系统中,每一个人包括其拥有的每一个物品都将随时随地连接到网络上,随时随地被感知,在这样的网络环境中,如何确保信息的安全性和隐私性,防止个人信息、业务信息和物品丢失或被他人盗用,将是物联网发展过程中需要解决的技术难题之一。

2.1.3 物联网的安全特征

物联网除了面临传统网络安全威胁以外,还具有一些特殊的安全问题。从物联网的信息处理过程来分析,感知信息经过采集、汇聚、融合、传输、决策和控制等过程,整个信息处理的过程,体现了物联网安全的特征和要求,因此,物联网安全与传统网络安全相比较,两者之间存在着较大的差别。物联网的安全特征如图 2-1 所示。

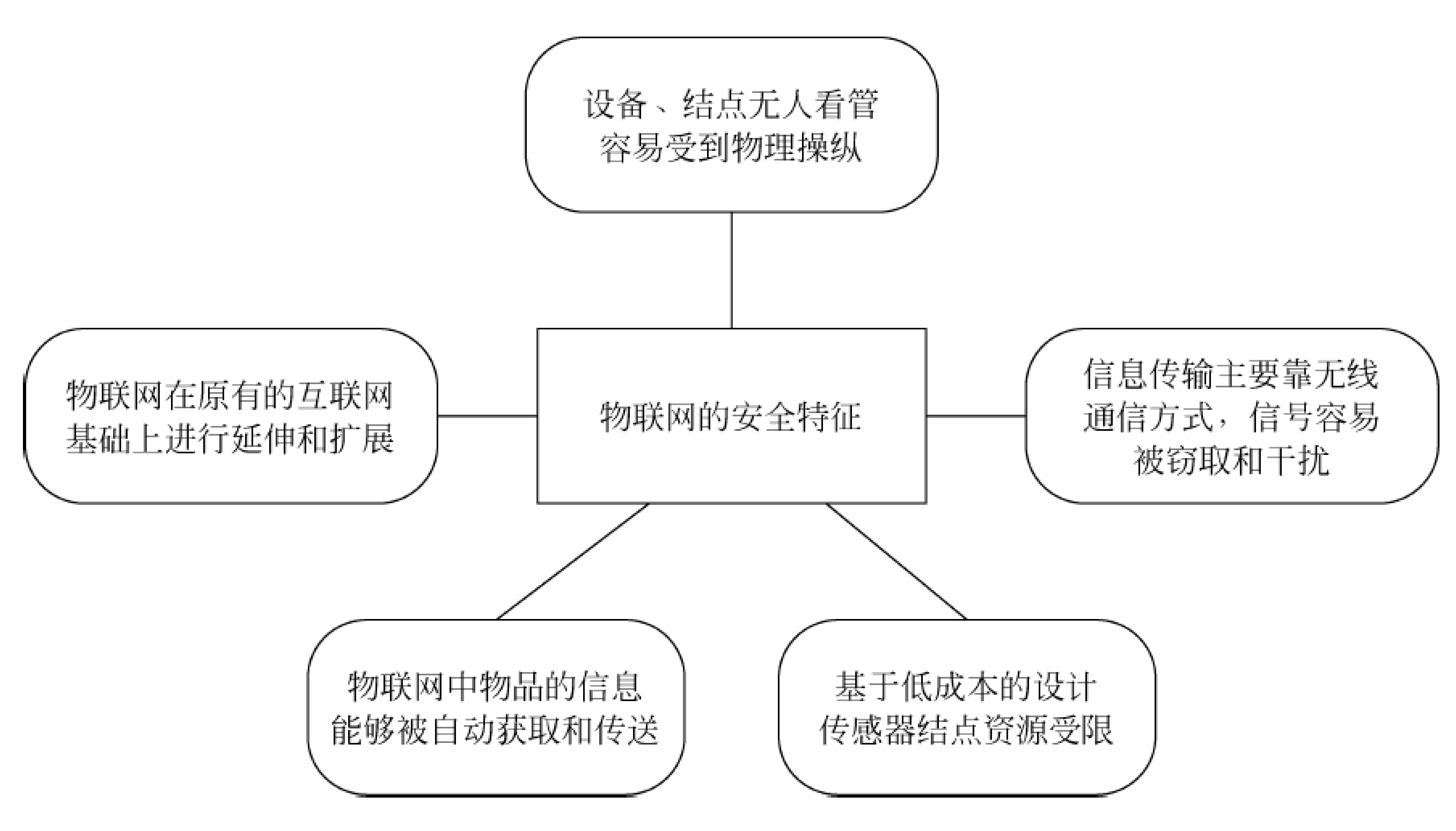


图 2-1 物联网的安全特征

1. 设备、结点无人看管,容易受到物理操纵

物联网常用来替代人完成一些复杂、危险和机械的工作。在这种工作环境下,物联网中的设备、结点都是无人看管的。因此,攻击者很容易就能接触到这些设备,从而对设备或者嵌入其中的传感器结点进行破坏。攻击者甚至可以通过更换设备的软硬件,对物联网进行非法操控。例如,在远距离电力输送过程中,供电企业可以使用物联网来远程操控一些供电设备。由于缺乏看管,攻击者有可能使用非法装置来干扰这些设备上的传感器。假如供电设备的某些重要工作参数被篡改,其后果不堪设想。

2. 信息传输主要靠无线通信方式,信号容易被窃取和干扰

物联网在信息传输中一般采用无线传输方式,暴露在空中的无线电信号很容易成为攻击者窃取和干扰的对象,这会对物联网的信息安全产生严重的威胁。例如,目前的第二代身份证都嵌入了 RFID 标签,在使用过程中,攻击者可以通过窃取感知结点发射的信号来获取

所需要的信息，甚至是用户的隐私信息，并据此来伪造身份，其后果非常严重。又如，攻击者可以在物联网无线电信号覆盖的区域内，通过发射无线电信号来进行干扰，从而使无线通信网络不能正常工作，甚至瘫痪。再如，在物流运输过程中，嵌入物品中的标签或读写设备的信号受到恶意干扰时，很容易造成一些物品的丢失。

3. 基于低成本的设计，传感器结点通常资源受限

在物联网的实际应用中，通常需要部署大量的传感器，以充分覆盖特定区域。对于已经部署的传感器，一般都不会进行回收或维护。因为具有数量多和一次性的特点，所以传感器必须具有较低的成本，只有这样，大规模使用才可行。为了降低成本，传感器通常是资源受限的。传感器一般体积较小，而且其能量、处理能力、存储空间、传输距离、无线电信号频率和带宽等都是受限的。由于以上各种原因，传感器结点无法使用比较复杂的安全协议，因此传感器设备或结点无法拥有较强的安全保护能力。攻击者针对传感器的这一弱点，可以采用连续通信的方式来使结点的能量耗尽。

4. 物联网中物品的信息能够被自动地获取和传送

物品的感知是物联网应用的前提。物品与互联网相连接后，通过射频识别(RFID)、传感器、二维识别码和 GPS 全球卫星定位等技术能够随时随地且自动地获取物品的信息。因此，人们随时随地都可以获取物品的准确位置和周围环境等相关信息。在物联网的应用中，RFID 标签可以被嵌入到任何物品中。一旦 RFID 标签被嵌入到人们的生活用品中，例如嵌入到帽子或衣服中，而使用者并没有察觉的话，那么物品的使用者将会被定位和跟踪，这无疑会对个人的隐私构成极大的威胁。

5. 物联网在原有的互联网基础上进行了延伸和扩展

物联网是在互联网基础上的延伸和扩展。与互联网相比较，物联网覆盖的范围更加广泛，包括了无处不在的数据感知、以无线电信号为主的信息传输、智能化的信息处理和广泛的应用，用户端可以延伸和扩展到任何物品与物品之间，进行信息的交换和通信。这样，使物联网安全的设计、部署和管理变得更为困难。

2.2 物联网安全体系结构

物联网安全的总体需求是物理安全、信息采集安全、信息传输安全和信息处理安全的综合，物联网安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性。

结合物联网的分布式连接和管理(Device Connect Manage，DCM)模式，可以得出物联网的安全体系结构，如图 2-2 所示。

正如本书的第 1 章所述，物联网的四个基本特征是：全面感知、可靠传输、智能处理和综合应用。

虽然人们对物联网的概念有多种不同的描述，但其内涵基本相同。因此，在分析物联网的安全性时，也相应地将其分为三个层次，即感知层安全、网络层安全和应用层安全。在物联网的综合应用方面，应用层是对智能处理后的信息的利用。尽管在某些物联网安全框架

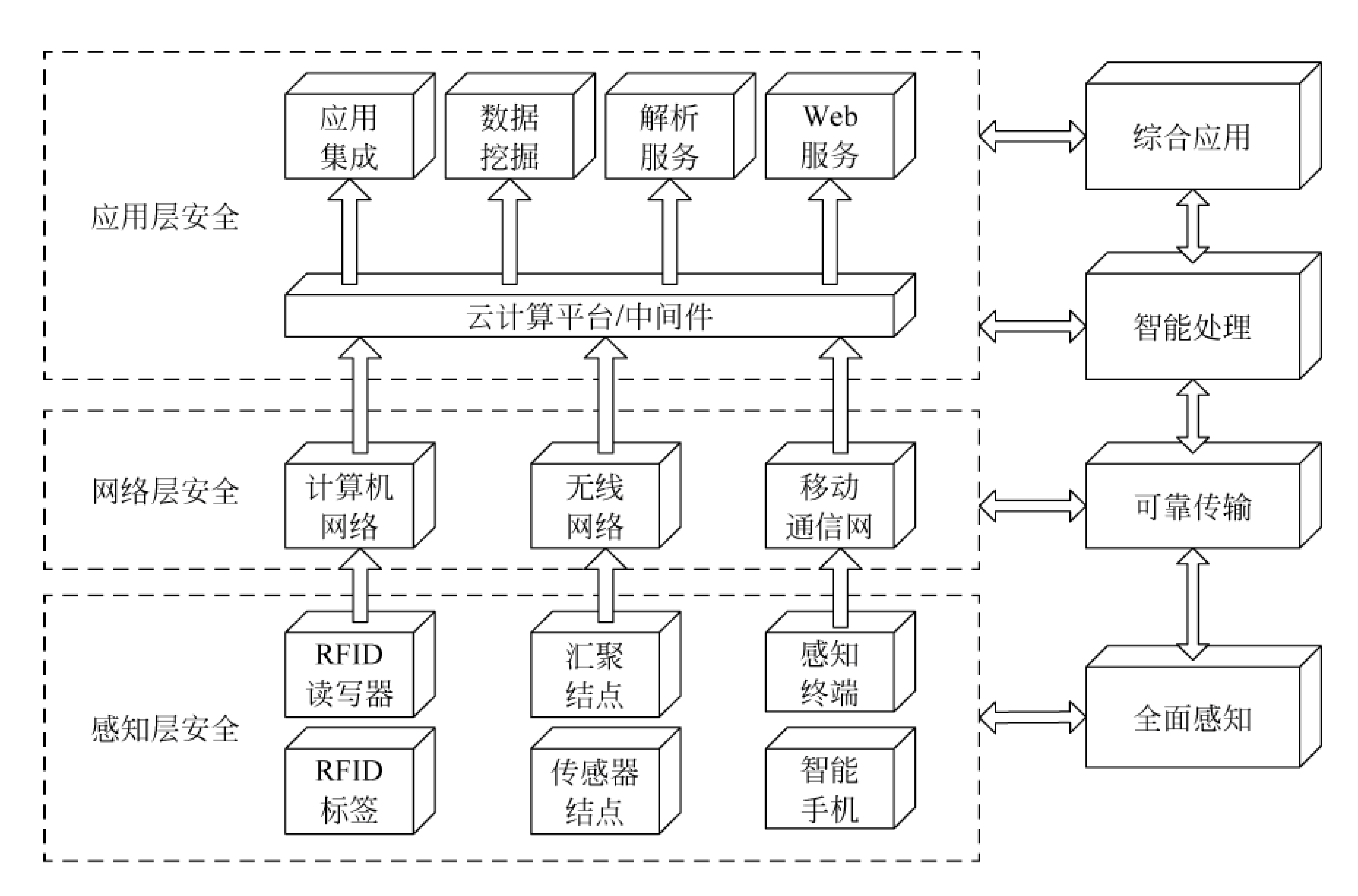


图 2-2 物联网安全的体系结构

中,将信息处理安全与信息应用安全分开进行分析,但是从物联网系统的整体信息安全角度来考虑,将这两者的安全问题统一到应用层,更容易建立物联网安全体系结构。

2.3 感知层安全分析

物联网感知层的任务是实现智能感知外界信息功能。感知层也可以称为原始信息收集层,包括信息采集、捕获和物体识别。该层的典型设备包括射频识别(Radio Frequency Identification,RFID)装置、各类传感器(如红外、声音、温度、湿度、速度等)、图像捕捉装置(摄像头)、全球定位系统(GPS)、激光扫描仪、环境检测仪和地震监测仪等。这些设备所收集的信息一般都具有明确的目的,所以在传统观念中这些信息直接被处理并进行应用。例如,公路边的摄像头捕捉的视频信息直接用于交通监控。然而,在物联网的应用中,多种类型的感知信息可能会同时处理、综合应用,甚至不同感应信息的结果会反馈给控制方,产生控制和调节行为。例如,湿度传感器收集到的湿度信息,可能会导致温度或光照程度的调节。同时,物联网应用强调的是信息共享,这是物联网区别于传感网的最大特点之一。又如,交通监控的录像信息可能同时被用于公安侦破、城市规划、环境监测等领域。因此,由什么部门来统一处理这些信息的问题将直接影响到应用的有效性。为了使这些信息能够被不同的应用领域共同分享并有效使用,应该有一个综合的物联网信息处理平台,这就是物联网的云计算平台。物联网感知的所有信息,都需要传输到这个统一的信息处理平台。

物联网的安全状况,主要体现在其体系结构的各个要素中。首先,是物联网的物理安全,这主要是各类传感器的安全,包括防范对传感器的干扰、屏蔽、电磁泄漏攻击、信道攻击等;其次,是物联网的运行安全,主要包括各个计算模块,如嵌入式计算模块、服务器的计算中心等,包括密码算法的实现、密钥管理(软件或硬件所存储的密钥)、数据接口和通信接口

管理等，涉及传感器结点、数据汇聚结点和数据处理中心；第三，是物联网的通信安全，即数据在传输过程中的安全保护，确保数据在传输过程中不会被非法窃取、篡改和伪造。

根据物联网感知层安全所涵盖的内容，可以把物联网的感知层分为两大类，即 RFID 系统和无线传感器网络。以下分别对这两类网络的安全技术进行分析。

2.3.1 RFID 系统安全分析

1. RFID 系统在安全防护方面的优势

RFID 射频识别是一种电子身份识别，其性质相当于条形码或二维码，但是它的功能却比条形码和二维码更强大。RFID 不仅提供电子身份标识，而且还具有少量的计算处理能力，因此，在安全防护方面，RFID 系统有着条形码和二维码不可比拟的优势。

RFID 系统一般包括一个或多个 RFID 电子标签，一个或多个读写器和一个后台数据库。读写器通过与后台数据库的交互，判断标签所提供的数据是否真实，RFID 标签也可以通过一些安全机制识别试图读取数据的读写器是否合法。RFID 标签与读写器之间的通信距离很短。尤其是无源标签，通常与读写器之间的通信距离只有几十厘米。而有源标签与读写器之间的通信距离，通常也仅仅在几十米之内，而且在很短的时间内就可以完成数据通信。

2. RFID 系统面临的安全问题

RFID 系统与无线传感器网络有着本质的区别。无线传感器网络传输的是采集得到的环境信息，当然也包括传感器自己的身份信息，而 RFID 标签仅仅传输一个身份标识信息。从表面上看，似乎 RFID 系统的工作机制要简单得多，然而实际的情况却并非如此。原因是 RFID 系统面临以下的安全问题：

1）非法复制

对于条形码或者二维码，非法复制是非常容易实现的；对于 RFID 系统，同样也会面对非法复制的问题，但是 RFID 系统应有能力对抗非法复制。

2）非法跟踪

非法读写器可能试图对合法的 RFID 标签进行访问，试图获得合法 RFID 标签的身份标识，从而可以判断该标签是否与在其他地方读取的 RFID 身份信息属于同一个标签。这种攻击的目的在于对某些标签实施跟踪。

3）限距离攻击

攻击者同时使用一对非法的 RFID 标签和读写器来实施攻击。首先使用非法的读写器接近一个合法的 RFID 标签，然后将该合法标签的数据传给远方的非法标签，该非法标签试图去接近一个合法的读写器，接着将非法读写器传来的信息发送给合法读写器，并将该合法读写器返回的任何信息传给远方的非法读写器，然后非法读写器返回给它接近的合法标签。通过这种攻击方式，将远处的非法标签与合法的读写器连接起来，似乎那个合法的标签在跟这个合法的读写器交互，从而试图通过认证。这种攻击行为是近年来提出的，其目的是通过 RFID 标签非法进入物联网系统。

RFID 标签的主要用途是识别某个账户或者某个物品，并且能够在数据库中记录该账

户或该物品的相关信息。非法复制是攻击者希望实现的，通过信息加密技术和物理保护措施，可以有效防止非法复制，起码可以使得非法复制的成本大大提高；即使不能非法复制，非法追踪 RFID 标签也是一种重要的攻击手段。因此，隐私保护是 RFID 系统安全的重要部分。此外，近年来提出的限距离攻击也对 RFID 系统安全提出了新的挑战。

3. RFID 系统安全技术

针对以上所描述的 RFID 系统的安全问题，其安全技术可以归纳为以下几点：

1）信息加密技术

通过信息加密技术，将 RFID 标签的机密信息存储在一个抗破解的硬件区域，可以有效地防止标签复制。同时，RFID 标签与读写器之间的信息交互过程也需要精心设计，否则在这些信息交互的过程中，有可能出现信息泄露。

2）身份隐私保护技术

通过加密措施，使标签提供给读写器的标识数据每次都产生变化，掌握机密信息的数据库可以识别该标签，但是作为非法截获数据的攻击者则无法识别这些不同的身份标识之间是否有关联，这样就可以避免标签被非法读写器识别，从而提供隐私保护机制。

3）抗限距离攻击技术

近年来，研究者们针对限距离攻击技术提出了许多解决方案，但是这些方案需要经过比较长时间的实践考验，才能确认是否可行，因此针对这种攻击行为的研究尚停留在实验室阶段。

2.3.2 无线传感器网络安全分析

当感知信息从传感器采集以后但尚未传输到网络层之前，可以把传感网本身（由各种传感器构成的网络）看作感知的部分。感知信息的传输要通过一个或多个与外部网络相连接的传感结点，这些结点称为网关结点（gateway）或汇聚结点（sink）。所有与传感网内部结点的通信，都需要经过网关结点与外部网络联系。因此，在物联网的感知层，我们仅仅需要分析传感网络本身的安全性即可。

1. 无线传感器网络面临的安全威胁

具有代表性的传感网是无线传感器网络，解决传感网安全的目标也应针对无线传感器网络，因为适合无线传感器网络的安全技术对有线传感网同样适合。以下分别对无线传感器网络面临的常见的安全威胁进行分析。

1）遭受非法用户的入侵

无线传感器网络最容易遭受的是非法用户的入侵，即使入侵失败，敌方反复地尝试入侵的过程，也可以造成对传感器结点的拒绝服务攻击。造成拒绝服务攻击的原因是无线传感器终端结点的资源有限，特别是采用电池供电的传感器结点，在不断对攻击者进行认证的过程中将会产生大量额外的功耗，从而造成电能耗尽。另外，在接收入侵请求的过程中，也可能造成自身计算超负荷而导致拒绝服务攻击。对汇聚结点而言，通常在能耗上没有太多的限制，绝大多数汇聚结点都可以保证电能的供应。但是，由于汇聚结点的设计是服务于少数传感器结点的，并且每一个传感器结点与汇聚结点之间的通信量一般都有限，因此汇聚结点

应对拒绝服务攻击的能力很弱，在拒绝服务攻击下也很容易导致计算资源耗尽。有时候，造成拒绝服务攻击后果的不一定是拒绝服务攻击，也可能是入侵尝试过程造成的拒绝服务攻击。当无线传感器网络被接入互联网，成为物联网系统的一部分时，受到拒绝服务攻击的机会将会大大增加。因此，感知层能否抵抗拒绝服务攻击，应作为一个健康的物联网系统的重要指标，这也是物联网安全面临的重要挑战。

2）被敌方非法捕获

由于无线传感器网络所处的环境一般都具有公开性，因此容易被敌方非法捕获。最容易被捕获的是传感结点发出的信号，这不需要知道它们的预置密码和通信密码，只需要鉴别传感结点的种类即可。例如，检查传感结点是用于检测温度还是用于检测噪声等。有时候这种分析对敌方也是很有用的。因此，安全的传感网络应该有保护其工作类型的安全机制。

3）被敌方剖析密钥

敌方不仅可以捕获无线传感器数据，而且可以捕获无线传感器网络的物理实体，然后进行离线分析，例如将数据带回实验室进行深入解剖，这样就有可能得到传感器所用的密钥信息，从而可以恢复该传感器之前的所有通信数据，甚至可能非法复制传感器，加入到传感网上发送虚假数据。

4）对汇聚结点的攻击

敌方对无线传感器网络更为严重的攻击是对汇聚结点的攻击。如果敌方能够控制汇聚结点，则不仅能得到所有该汇聚结点所服务的传感结点上传的所有数据，而且可以任意制造虚假的数据，甚至可以蒙骗数据处理中心和感知终端。敌方对汇聚结点的安全性分析，不一定需要到实验室进行硬件解剖，更多的是根据传感网所使用的认证安全技术，通过协议漏洞和其他方面可能的漏洞分析，找到成功入侵的机会，一旦入侵成功，就可以对汇聚结点实施所有可能的攻击，例如解密数据、捏造数据等，并有可能导致服务器端的故障。

2. 无线传感器网络的安全技术

针对以上所描述的安全威胁，无线传感器网络的安全技术可以归纳为以下几点：

1）结点认证

结点认证包括传感器结点与传感器结点之间、传感器结点与汇聚结点之间的单向和双向认证，确保信息的来源和去向正确，以防假冒攻击。

2）消息机密性

所谓消息的机密性是保护数据不被非法截获者获知。在实施过程中，需要考虑密钥管理问题。在传感网络使用公钥系统是不容易实现的，因为公钥系统所消耗的计算资源太多，而且公钥基础设施在传感网中无法运转起来。假如使用对称密钥，无论是给每一个传感结点赋予一个单独的密钥，还是让一个传感网内的所有结点共享一个预置密钥，都是现实中需要考虑的问题。

3）数据完整性

数据的完整性是保护传输的数据不被非法修改，同时有效地拒绝敌方制造的假信息。

4）数据新鲜性

如果说在互联网中数据的新鲜性保障不是很强的话，在传感网络中则需要保障数据的新鲜性。一方面，传感器结点上传的数据具有很高的时效性甚至实时性；另一方面，从数据

中心传给传感器结点的消息通常都是重要的控制指令，如果仅仅保证机密性和完整性，并不能完全满足要求。因为简单的重放攻击可以通过消息机密性和数据完整性验证，从而可能会造成很大的问题，例如控制开关的开启或者关闭指令的重放，就有可能导致非常严重的后果。

5）安全路由

安全路由在一些传感网络中非常重要，但并不是所有的传感网络都需要安全路由。许多物联网行业中使用的传感网络根本就不需要路由，传感器结点可以直接将感知数据传送给汇聚结点。

6）密钥管理

尽管传感网络大多使用对称密钥技术，但是在资源有限的环境中，对密钥的有效和安全管理同样具有技术挑战性。如果在汇聚结点和传感器结点使用同一个密钥，虽然有利于物联网系统的搭建，但是只要敌方控制传感网络中的一个传感器结点，则整个传感网将不再具有安全性；如果在每个传感器结点使用一个不同的密钥，则增加了汇聚结点的计算工作量，汇聚结点需要管理所有结点对应的密钥。此外，汇聚结点也处于相对公开的环境，容易遭受入侵甚至物理攻击，因此，这些与传感器结点共享的密钥，无论是长期保存还是临时存放，都是对物联网安全技术的挑战。

7）抗拒绝服务攻击

拒绝服务攻击并不是互联网独有的，在传感网中实施拒绝服务攻击更加容易。每当出现某个访问请求，接收结点需要对该请求进行一系列的认证过程，许多同样的请求将导致许多次重复的过程，对一个处理能力不强的汇聚结点而言，很容易造成计算超出负荷，从而导致拒绝服务；对于计算能力更弱的一个普通传感结点来说，就更容易导致瘫痪，甚至电能耗尽。对于传感结点来说，对抗拒绝服务攻击的有效手段是采取适当的睡眠机制。但是对于汇聚结点，睡眠机制是否有效还有待进一步的研究。

2.3.3 感知层安全机制

在物联网感知层，需要提供消息机密性、数据完整性和认证等安全机制，然而物联网感知层的感知结点受资源所限，常常只能执行少量的计算和通信任务。特别地，对于一些资源非常受限的感知结点（包括传感器结点和 RFID 标签），如何提供所需要的安全机制面临着许多的技术挑战。为此，针对物联网感知层的安全，需要轻量级加密算法和轻量级安全认证协议。

随着移动电子设备的普及和 RFID、无线传感器网络等技术的发展，越来越多的应用需要解决相应的安全问题。但是，相对于传统的台式和高性能的计算机，这些移动设备的资源环境通常有限，存在着计算能力比较弱、计算时可以使用的内存空间比较少以及能耗有限的问题。传统的加密算法并不能很好地应用于这种环境，这样就使得在受限环境中加密算法的研究，成为当前一个迫切需要解决的热点问题。适用于资源受限环境中的加密算法称为轻量级加密算法。

轻量级加密算法与传统加密算法互相促进，互相影响。一方面，传统加密算法为轻量级加密算法的设计与安全性分析提供了理论依据和技术支持；另一方面，轻量级加密算法的“轻量级”特点，使传感器网络的安全性分析能够更加深入、全面地展开。在这个过程中，可

能会出现新的问题，从而促进加密算法和安全技术的发展。

物联网的感知层安全需要轻量级加密算法，以适应资源受限的感知结点的环境需求。然而，到底什么是轻量级并没有严格的定义，也很难给出严格的定义。根据国际 RFID 标准委员会的规定，RFID 标签需要留出 2000 个门电路和相当的硬件资源用于加密算法的实现。因此，研究者通常把轻量级加密算法定义为那些在 2000 个门电路硬件资源之内可以实现的加密算法。准确地说，2000 个门电路硬件资源仅仅是一个供参考的性能技术指标，实际上轻量级加密算法允许有不同的性能技术指标，某些感知结点对硬件资源的限制可能更为苛刻，而另外一些感知结点则允许使用更多的硬件资源。

基于物联网技术的发展，近年来，轻量级加密算法引起了研究者和业界的广泛关注。轻量级加密算法逐步从实验室迈向实用阶段。轻量级加密算法设计的关键问题是处理安全性、实现代价和性能之间的平衡。

当前，实现 RFID 系统安全机制的方法主要有三大类：物理安全机制、密码安全机制以及二者的结合。

物理安全机制主要包括杀死机制、休眠机制、阻塞机制、静电屏蔽、主动干扰等方法；密码安全机制主要包括哈希锁协议、随机哈希锁协议、哈希链协议、哈希函数构造算法、基于矩阵密钥的认证协议、数字图书馆协议等。

RFID 系统的物理安全机制和密码安全机制将在本书第 4 章进一步分析。

2.4 网络层安全分析

2.4.1 网络层面临的安全挑战

物联网的网络层主要用于把感知层收集到的信息安全可靠地传输到应用层，然后根据不同的应用需求进行信息处理，即网络层主要提供信息传输所用的网络基础设施，包括互联网、移动通信网和一些专用网络。在信息传输过程中，可能需要经过一个或多个不同架构的网络进行信息交换。例如，手机与固定电话机之间的通话就是一个典型的跨网络架构的信息传输实例。在传统的信息传输过程中，跨越不同类型网络的信息传输是很正常的，在物联网环境中，这种传输方式变得更为典型，并且很可能在传输过程中产生信息安全隐患。

物联网网络层涉及移动通信网、国际互联网和无线网络等多种不同的网络环境。

移动通信网络的发展早已超越了提供语音服务的原始用途。以智能手机为代表的移动设备的普及，也给移动通信网络不断地提出新的需求。目前移动通信网络所提供的服务主要包括移动互联网、多媒体服务、互动游戏、网络聊天等。因此，对移动通信网络的攻击也远远超越了窃听语音的范围。

在物联网中，当前的 IPv4 网和下一代的 IPv6 网都是物联网信息传输的核心载体，绝大多数信息要经过互联网传输。传统的互联网受到的拒绝服务攻击（DoS 攻击）和分布式拒绝服务攻击（DDoS 攻击）依然存在，因此需要有更好的防范措施和灾难恢复机制。由于物联网所连接的终端设备性能和对网络需求存在着巨大差异，对网络攻击的防护能力也会有很大差别，因此很难设计通用的安全方案，而应针对不同的网络安全需求采取不同的解决方案。

物联网中感知层所获取的感知信息通常由无线传感器网络传输到系统。与互联网相比，恶意程序在无线网络环境和传感网络环境中有很多入口。对这些暴露在公共场所之中的感知信息，如果不进行合理的保护，就很容易被入侵。例如，类似于蠕虫病毒这种恶意代码一旦入侵成功，其隐蔽性、传播性和破坏性等更加难以防范，在这样的环境中检测和清除这类恶意代码将更加困难，这直接影响到物联网系统的安全性。物联网建立在互联网的基础上，对互联网的依赖性很高，在互联网中存在的危害信息安全的因素，在一定程度上同样也会造成对物联网的危害。随着物联网的发展，病毒攻击、黑客入侵、非法授权访问等都会对物联网用户造成损害。

总之，传统的互联网网络环境遭遇到前所未有的安全挑战，而物联网网络层所处的网络环境也同样存在安全隐患。与此同时，由于不同架构的网络需要相互连通，因此在跨网络架构的安全认证方面会面临更大的挑战。

2.4.2　网络层安全分析

在网络层，异构网络的信息交换将成为安全性的脆弱点，尤其是在网络认证方面，难免出现中间人攻击和其他类型的攻击。针对这些攻击，都需要有更高的安全防护措施。如果仅仅考虑互联网和移动网以及其他一些专用网络，则物联网网络层对安全的需求可以概括为以下几个方面。

1. 数据机密性

数据机密性指网络层需要保证数据在传输过程中不泄露其内容。

2. 数据完整性

数据完整性指网络层需要保证数据在传输过程中不被非法篡改，或者非法篡改的数据很容易被检测出来。

3. 数据流机密性

数据流机密性指在网络层的应用环境中，需要对数据流进行保密。

4. 分布式拒绝服务攻击的检测与防护

物联网网络层需要解决如何对脆弱结点的分布式拒绝服务攻击进行检测与防护。

5. 跨区域、跨网络认证机制

跨区域、跨网络认证机制包括不同类型的网络所使用的跨区域认证、跨网络认证机制。

2.4.3　网络层的安全机制

物联网网络层的安全机制，可以分为端到端的机密性和结点到结点的机密性。

端到端的机密性，需要建立以下安全机制：端到端认证机制、端到端密钥协商机制、密钥管理机制和机密性算法选择机制等。在这些安全机制中，按需要可以增加数据完整性

服务。

结点到结点的机密性,需要结点间的认证和密钥协商协议,这一类协议要重点考虑效率因素。机密性算法的选择和数据完整性服务,可以根据需求选取或省略。由于存在跨网络架构的安全需求,因此需要建立不同网络环境的认证衔接机制。此外,根据应用层的不同需求,网络传输模式可以区分为单播通信、组播通信和广播通信。针对不同类型的通信模式,也应当有相应的认证机制和机密性保护机制。

2.5 应用层安全分析

2.5.1 云计算平台安全

1. 云计算平台概述

物联网应用层的任务就是对感知数据的处理与应用。从物联网的行业应用来分析,应用层必须具有一定规模的信息处理中心和应用平台,否则不能承担起物联网各种行业应用的重担。为了支持物联网产业的发展,目前,许多国家和地区都建立了各自的云计算平台,因此物联网应用层的安全机制主要是针对云计算平台而言的。

作为物联网应用层基础设施的云计算平台,应当具有能力处理海量数据。并且,云计算平台除了需要具有很强大的信息处理能力以外,还必须具有备份和抗击灾害等能力;云计算平台应能够应对大量不同用户的访问,而这种访问不同于普通的网站,需要为用户提供私有数据空间和私有计算处理能力,因此虚拟化成为云计算的典型特征;云计算平台将难免遭受各类网络攻击和系统安全的威胁,因此云计算平台必须具有抗攻击和抗病毒的能力。

2. 云计算面临的安全挑战

云计算的重要特征是智能,智能的技术实现少不了自动处理技术,其目的是使处理过程方便快捷,而非智能的处理手段可能无法应对海量数据。但是在自动处理的过程中,对恶意数据特别是恶意代码的判断能力是有限的,而智能也仅限于按照一定规则进行过滤和判断,因此攻击者很容易避开这些规则。例如,对于垃圾电子邮件的过滤就是一个多年无法彻底解决的棘手问题。制定防御规则时需要考虑尽可能多的攻击手段,而攻击者只需要应对已知的规则。云计算面临的安全挑战主要包括以下几个方面。

(1) 来自于超大量终端的海量数据的识别和及时处理。

(2) 智能是否会被敌方利用。

(3) 自动是否会变为失控。

(4) 灾难控制和恢复能力。

(5) 如何杜绝非法攻击。

由于在物联网时代需要处理的信息是海量的,云计算平台也是分布式的,因此当不同性质的数据通过一个云计算平台处理时,这个云计算平台需要多个功能各异的处理平台协同处理。但是首先应该知道将哪些数据分配到哪个处理平台,因此数据的分类是必需的。同时,基于安全性的要求使得许多信息都是以加密形式存在的,因此如何快速有效地处理海量

加密数据是智能处理阶段遇到的一个重大挑战。

3. 云计算平台的安全机制

云计算技术的智能处理过程与人类的智能相比还是有本质的区别，但是计算机的智能判断在速度上是人类智力判断所无法比拟的。因此，基于物联网环境的云计算技术，在智能处理的水平上有望不断提高。反过来说，只要智能处理过程存在，就有可能让攻击者躲过智能处理的识别和过滤，从而达到攻击的目标。因此，物联网的云计算平台需要高智能的处理机制。

如果智能水平很高，那么就可以有效识别并自动处理恶意数据和指令。但是再好的智能也会存在失误的可能，特别是在物联网环境中，即使失误概率非常小，因为自动处理过程的数据量非常庞大，所以失误的情况还是难以避免。在处理发生失误而使攻击者成功入侵后，如何将攻击所造成的损失降到最低程度，并尽快使系统从灾难中恢复到正常工作状态，是物联网智能应用层需要解决的另一个重要问题。

云计算虽然使用智能的自动处理手段，但是还是允许人工干预，而且人工干预在某些时候是必需的。人工干预往往发生在智能处理过程中无法做出正确判断的时候，也可能发生在智能处理过程中出现关键性中间结果或最终结果的时候，还可能发生在任何其他原因而需要人工干预的时候。人工干预的目的是为了使应用层更好的工作。此外，由于来自于人的恶意破坏行为具有很大的不可预测性，因此针对人类的恶意破坏行为，除了采用技术手段以外，还需要依靠严格和科学的管理手段。

为了实现物联网云计算的安全需求，需要提供以下的安全机制。

(1) 可靠的认证机制和密钥管理方案。

(2) 高强度数据机密性和完整性服务。

(3) 可靠的密钥管理机制。

(4) 密文查询、秘密数据挖掘、安全云计算技术。

(5) 可靠和高智能的处理能力。

(6) 抗网络攻击，具有入侵检测和病毒检测能力。

(7) 恶意指令分析与预防，访问控制及灾难恢复机制。

(8) 保密日志跟踪和行为分析，恶意行为模型的建立。

(9) 具有数据安全备份、数据安全销毁以及流程全方位审计能力。

(10) 移动设备的识别、定位和追踪机制。

2.5.2 物联网应用层安全分析

物联网应用层行业应用的设计目标，是针对某个具体行业的综合性的或者个性化的应用业务。行业应用所涉及的安全问题，仅仅通过感知层、网络层、应用层这三层的安全解决方案，仍然有可能无法解决。在这些安全问题中，隐私保护就是一个典型的应用需求。无论是感知层、网络层还是应用层，都没有涉及隐私保护问题，但是它却是物联网的特殊应用环境中的实际需求，即应用层的特殊安全需求。还有，物联网的数据共享分多种情况，涉及不同权限的数据访问。另外，物联网应用层还涉及知识产权保护、计算机数据取证、计算机数据销毁等安全需求及相关技术。

1．应用层行业应面临的安全挑战

物联网应用层的安全需求和安全挑战主要来自以下几个方面。

（1）根据不同访问权限对同一数据库的内容进行筛选。

（2）既能提供用户隐私信息保护，同时又能正确认证。

（3）解决信息泄露和追踪问题。

（4）进行计算机数据取证。

（5）销毁计算机数据。

（6）保护电子产品和软件的知识产权。

物联网需要根据不同的应用需求对共享数据分配不同的访问权限，并且不同权限访问同一数据时可能得到不同的结果，例如，当道路交通监控视频数据用于城市规划时仅仅需要很低的分辨率，因为城市的规划需要的是交通拥塞的大致情况；而监控视频用于交通管制时分辨率就需要清晰一些，因为需要准确地知道交通实际情况，及时发现究竟哪里发生了交通事故，以及交通事故的基本情况等；当监控视频用于公安侦查时可能需要更高的分辨率，以便于看清楚人的身材和外貌或者识别汽车牌照等信息。因此，如何以安全方式处理信息是物联网应用中的一项挑战。

在很多情况下，用户信息是认证过程中的必需信息，如何为这些信息提供隐私保护，是一个必须解决的安全问题。

随着商业信息和个人信息的网络化，越来越多的信息被认为是用户隐私信息。需要隐私保护的应用至少应包括以下几种。

（1）移动用户既需要知道自己的位置信息，又不愿意非法用户获取该信息。

（2）物联网用户既需要证明自己有权合法使用某种业务，又不想让别人知道自己在使用这种业务，例如金融交易、在线游戏等。

（3）许多物联网业务需要匿名操作，例如网络投票。

（4）在医疗管理系统中，需要保存病人的相关信息，以便于医生诊病时获取正确的病例数据，但又要避免这些病例数据跟病人的身份信息相关联。在这种情况下，应当通过加密技术对病人病历的隐私信息加以保护。

在互联网环境的商业活动中，无论采用什么技术，都难以避免恶意行为的发生。假如能够根据恶意攻击行为所造成的后果的严重程度给予相应的惩罚，则可以减少恶意行为的发生。在技术上，就需要收集相关的犯罪证据。因此，计算机取证就显得非常重要。然而计算机取证具有较大的技术难度，原因是计算机平台的种类太多，包括多种计算机操作系统和智能设备操作系统等。

与计算机取证相对应的是计算机数据销毁。数据销毁的目的是销毁那些在密码算法和密码协议实施过程中所产生的临时中间变量，一旦加密算法和密码协议实施完成，这些中间变量将不再有用。但是这些中间变量如果落入攻击者手中，就有可能为攻击者提供重要的资料，从而提高成功攻击的可能性。因此，这些临时中间变量需要及时地从计算机内存和硬盘存储空间中删除。同时，计算机数据销毁技术也有可能为计算机犯罪者提供证据销毁工具，从而增大计算机取证的难度。如何处理好计算机取证与计算机数据销毁这对矛盾，也是物联网应用中需要解决的安全问题。

2. 物联网应用层安全机制

物联网的典型应用是商业应用，在商业应用中存在着大量需要保护的知识产权产品，包括专利、商标、软件和电子产品等。在物联网应用中，对电子产品的知识产权的保护将会提高到一个新的高度，对相应的安全技术要求也是一项新的挑战。

基于物联网应用层的安全需求和安全挑战，需要实现以下的安全机制。

(1) 有效的数据库访问控制和内容筛选机制。

(2) 不同应用场景中的隐私信息保护技术。

(3) 叛逆追踪和其他信息泄露追踪机制。

(4) 有效的数据取证技术。

(5) 安全的数据销毁技术。

(6) 安全的电子产品和软件的知识产权保护技术。

针对物联网应用层的这些安全机制，需要提供相应的加密技术，包括访问控制、匿名签名、匿名认证、密文验证、门限密码、叛逆追踪、数字水印和数字指纹技术等。

2.6 本章小结

物联网安全是指物联网系统可以连续地、可靠地和正常地运行，服务不会中断，物联网系统中的软件、硬件和系统中的数据受到保护，不受人为的恶意攻击、破坏和更改。

互联网技术是物联网的基础，互联网的安全直接关系到整个物联网的安全。互联网安全问题涉及网络设备基础安全、网络安全、Web 安全和基于 Web 应用的安全等各个方面，包括安全编码、数据帧安全和密钥管理与交换等。

物联网是由大量的传感器等设备构成的，缺少人对设备的有效监控，并且物联网设备种类繁多、数量庞大，所以物联网还面临其特有的安全威胁。包括点到点消息认证、重放攻击、拒绝服务攻击、篡改或泄漏标签数据、权限提升攻击、业务安全和隐私安全等。

物联网安全的特点包括设备、结点无人看管，容易受到物理操纵；信息传输主要靠无线通信方式，信号容易被窃取和干扰；基于低成本的设计，传感器结点通常是资源受限的；物联网中的物品的信息能够被自动地获取和传送；物联网在原有的网络基础上进行了延伸和扩展。

物联网安全的体系结构包括信息采集安全、信息传输安全、信息处理安全和信息应用安全。

根据物联网感知层安全所涵盖的内容，可以把物联网的感知层分为两大类，即传感网和RFID 系统。针对物联网感知层的安全，需要轻量级加密算法和轻量级安全认证协议。

物联网网络层涉及移动通信网、国际互联网和无线网络等多种网络环境。物联网网络层的安全机制，可以分为端到端的机密性和结点到结点的机密性。

代表着物联网应用层的云计算平台，除了需要有能力处理海量数据，还必须具有备份和抗击灾害等能力，能为用户提供私有数据空间和私有计算处理能力，并且具有抗攻击和抗病毒的能力。

物联网的典型应用是商业应用，在商业应用中存在着大量需要保护的知识产权产品，包

括专利、商标、软件和电子产品等。针对物联网应用层的安全机制，需要提供相应的加密技术，包括访问控制、匿名签名、匿名认证、密文验证、门限密码、叛逆追踪、数字水印和数字指纹技术等。

复习思考题

1. 物联网安全的含义是什么？
2. 传统网络面临哪些安全威胁？
3. 物联网面临哪些特有的安全威胁？
4. 请分析物联网的安全特征。
5. 请画图描述物联网安全的体系结构。
6. 请简要分析无线传感器网络的安全威胁。
7. 请简要分析 RFID 系统的安全威胁。
8. 请简要说明物联网感知层的安全机制。
9. 请简要说明物联网网络层的安全机制。
10. 请简要说明物联网云计算平台的安全机制。
11. 请简要说明物联网应用层的安全机制。

第3章 信息安全技术基础

3.1 密码学概论

密码学(cryptography)是一门古老而深奥的学科,它以认识密码变换为本质,以加密与解密基本规律为研究对象。Cryptography 一词来源于古希腊的 crypto 和 graphen,意思是密写。保密通信的思想和方法早在几千年前就已经有了,埃及人是最先使用特别的象形文字作为信息编码的人。随着时间推移,巴比伦、美索不达米亚和希腊都开始使用一些方法来保护他们的书面信息。对信息进行编码曾被凯撒大帝(Julias Caesar)使用,也曾用于历次战争中,包括美国独立战争、美国内战和两次世界大战。最广为人知的加密机器是德国的 Enigma 机,在第二次世界大战中德国人利用它创建了加密信息。此后,由于 Alan Turing 和 Ultra 计划以及其他人的努力,终于对德国人的密码进行了破解。当初,计算机的研究就是为了破解德国人的密码,人们并没有想到计算机给今天带来的信息技术革命。近年来,密码学研究之所以十分活跃,主要是它与计算机科学的蓬勃发展密切相关;此外,还有在电信、金融领域和防止日益广泛的计算机犯罪的需要。在互联网出现之前,密码技术已经广泛应用于军事和民用方面。现在,密码技术在计算机网络中的应用实例越来越多。

3.1.1 密码学的历史

密码学的发展历程大致经历了三个阶段:古代加密方法、古典密码和近代密码。

1. 古代加密方法(手工阶段)

这一时期的密码技术源于战争需求,可以说是一种艺术,而不是一种科学。存于石刻或史书中的记载表明,许多古代文明,包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说,战争是科学技术进步的催化剂。人类自从有了战争,就面临着通信安全的需求,密码技术历史悠久、源远流长。古代加密方法大约起源于公元前 440 年,出现在古希腊战争中的隐写术,当时为了安全传送军事情报,奴隶主剃光奴隶的头发,将情报写在奴隶的光头上,待头发长长后将奴隶送到另一个部落,再次剃光头发,原有的信息复现出来,从而实现这两个部落之间的秘密通信。

我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式,将要表达的真正意思或“密语”隐藏在诗文或画卷中特定位置的记载,一般人只注意诗或画的表面意境,而不会去注意

或很难发现隐藏其中的“话外之音”。比如,我画蓝江水悠悠,爱晚亭上枫叶愁。秋月溶溶照佛寺,香烟袅袅绕轻楼(藏头诗)。

最早的密码技术,来源于公元前2000年。希伯来人的一种加密方法是把字母表调换顺序,这样的字母表的每一个字母就被映射成调换顺序后的字母表中的另一个字母,这种加密方法被称为atbash。例如,单词security就被加密成hvxfirgb,这是一种代换密码,因为一个字母被另一个字母所代替。这种代换密码被称为单一字母替换法,因为它只使用一个字母表,而一次用多个字母表的加密方法,则称为多字母替换法。公元前400年,斯巴达人就发明了“塞塔式密码”,即把长条纸螺旋形地斜绕在一个多棱棒上,将文字沿棒的水平方向从左到右书写,写一个字旋转一下,写完一行再另起一行从左到右写,直到写完。解下来后,纸条上的文字消息杂乱无章、无法理解,这就是密文,但将它绕在另一个同等尺寸的棒子上后,就能看到原始的消息。

后来,朱丽叶斯·凯撒发明了一种近似于atbash替换字母的方法。当时,没多少人能够第一时间读懂,这种方法提供了较高的机密性。中世纪,欧洲人在不断利用新的方法、新的工具和新的实践优化自己的加密方案。在19世纪晚期,密码学已经被广泛地用作军事上的通信方法。

2. 古典密码(机械阶段)

古典密码的加密方法一般是文字置换,使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形,它比古代加密方法复杂,其变化较小。随着机械和电子技术的发展,电报和无线通信的出现,加密装置得到了突飞猛进的提高,转子加密机是军事密码学上的一个里程碑,这种加密机是在机器内用不同的转子来替换字母,它提供了很高的复杂性,从而很难攻破。

德国的Enigma机是历史上最著名的加密机,如图3-1所示。这种机器有三个转子、一个线路连接板和一个反转转子。在加密过程开始之前,消息产生者将Enigma机配置成初



图3-1 Enigma机

始设置,操作员把消息的第一个字母输入加密机,加密机用另一个字母来代替并把这个字母显示给操作员看。它的加密机制是:通过把转子旋转预定的次数用另一个不同的字母来代替原来的字母。因此,如果操作员把 T 作为第一个字符敲入机器中,Enigma 机可能会把 M 作为密文,操作员把就字母 M 写下来,然后他可以加快转子的速度再输入下一个字符,每加密一个字符操作员就加快转子的速度作为一个新的设置。继续这样下去,直到整个消息被加密。然后,加密的密文通过电波传输,大部分情况是传到潜水艇。这种对每个字母有选择性地替换依赖于转子装置,因此这个过程的关键和秘密的部分(密钥)在于在加密和解密的过程中操作员是怎样加速转子的。两端的操作员需要知道转子的速度增量顺序以使得德国情报部门能够正确地通信。尽管 Enigma 机的装置在当时非常复杂,但还是被一组波兰密码学家攻破,从而使得英国知道了德国的进攻计划和军事行动。有人说,Enigma 机的破译使第二次世界大战缩短了两年。

3. 近代密码(计算机阶段)

前面介绍了古代加密方法和古典密码,它们的研究还称不上是一门科学。直到 1949 年香农发表了一篇题为"保密系统的通信理论"的著名论文,该文首先将信息论引入了密码,从而把已有数千年历史的密码学推向了科学的轨道,奠定了密码学的理论基础。该文利用数学方法对信息源、密钥源、接收和截获的密文进行了数学描述和定量分析,提出了通用的密钥密码体制模型。

需要提出的是,由于受历史的局限,20 世纪 70 年代中期以前的密码学研究基本上是秘密地进行,而且主要应用于军事和政府部门。密码学的真正蓬勃发展和广泛的应用是从 20 世纪 70 年代中期开始的。1977 年美国国家标准局颁布了数据加密标准 DES 用于非国家保密机关。该系统完全公开了加密、解密算法。此举突破了早期密码学的信息保密的单一目的,使得密码学得以在商业等民用领域的广泛应用,从而给这门学科以巨大的生命力。

在密码学发展的进程中的另一件值得注意的事件是,在 1976 年,美国密码学家迪菲和赫尔曼在一篇题为"密码学的新方向"一文中提出了一个崭新的思想,不仅加密算法本身可以公开,甚至加密用的密钥也可以公开。但这前不意味着保密程度的降低。因为如果加密密钥和解密密钥不一样,只要将解密密钥保密仍然可以实现加密,这就是著名的公钥密码体制。若存在这样的公钥体制,就可以将加密密钥像电话簿一样公开,任何用户当它想经其他用户传送一加密信息时,就可以从这本密钥簿中查到该用户的公开密钥,用它来加密,而接收者能用只有他自己知道的解密密钥得到明文。任何第三者都不能获得明文。1978 年,由美国麻省理工学院的里维斯特,沙米尔和阿德曼提出了 RSA 公钥密码体制,它是第一个成熟的、迄今为止理论上最成功的公钥密码体制。它的安全性是基于数论中的大整数因子分解。该问题是数论中的一个困难问题,至今没有有效的算法,这使得该体制具有较高的保密性。

按照人们对密码的一般理解,密码是用于将信息加密而不易破译,但在现代密码学中,除了信息保密外,还有另一方面的要求,即信息安全体制还要能抵抗对手的主动攻击。所谓主动攻击指的是攻击者可以在信息通道中注入他自己伪造的消息,以骗取合法接收者的相信。主动攻击还可能窜改信息,也可能冒名顶替,这就产生了现代密码学中的认证体制。该体制的目的就是保证用户收到一个信息时,他能验证消息是否来自合法的发送者,同时还能验证该信息是否被窜改。在许多场合中,如电子汇款,能对抗主动攻击的认证体制甚至比信

息保密还重要。

在密码学的发展过程中，数学和计算机科学至关重要。数学中的许多分支如数论、概率统计、近世代数、信息论、椭圆曲线理论、算法复杂性理论、自动机理论、编码理论等都可以在其中找到各自的位置。

密码形成一门新的学科是受计算机科学蓬勃发展刺激和推动的结果。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，另一方面也给破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸进行手工设计时易犯的错误，也不用再面对用电子机械方式实现的密码机的高额费用。总之，利用电子计算机可以设计出更为复杂的密码系统。

3.1.2 密码系统的概念

密码系统又称为密码体制，是指能完整地解决信息安全中的机密性、数据完整性、认证、身份识别及不可抵赖等问题中的一个或几个的一个系统。其目的是人们能够使用不安全信道进行安全的通信，如图 3-2 所示。

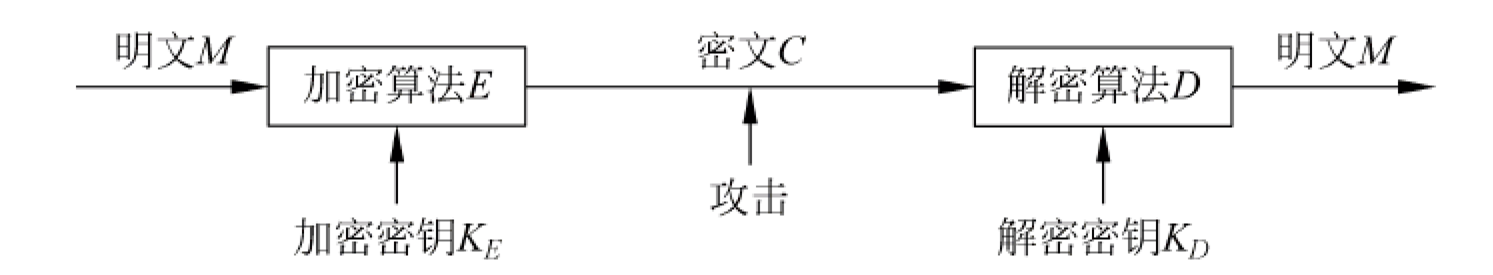


图 3-2 密码系统

一个密码系统由算法以及所有可能的明文、密文和密钥组成。因此，一个完整的密码体制要包括如下五个要素{M,C,K,E,D}：

(1) M，明文(Plain-text)是明文的有限集，称为明文空间；

(2) C，密文(Cipher-text)是密文的有限集，称为密文空间，是对明文变换的结果；

(3) K，密钥(Key)是一切可能的密钥构成的有限集，称为密钥空间；

(4) E，加密算法(Encrypt)是一组含有参数的变换；

(5) D，解密算法(Decrypt)加密的逆变换。

密码体制的设计要求应符合早在 1883 年由科克霍夫斯(A. Kerchoffs)提出的一个重要原则：密码系统中的算法即使为密码分析者所知，也无助于用来推导出明文和密文。

密码体系的加密过程描述：$C= K_E(M)$

密码体系的解密过程描述：$M= K_D(C)$

3.1.3 密码的分类

从不同的角度根据不同的标准，可以把密码分成若干类。

1. 按应用技术或历史发展阶段划分

(1) 手工密码。以手工完成加密操作或者以简单器具辅助操作的密码，称为手工密码。第一次世界大战前主要是这种操作形式的密码。

(2) 机械密码。以机械密码机或电动密码机来完成加解密操作的密码，称为机械密码。

这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

(3) 电子机内乱密码。通过电子电路以严格的程序进行逻辑运算,以少量制乱元素生产大量的加密乱数,因为其制乱是在加解密过程中完成的而无须预先制作,所以称为电子机内乱密码。从 20 世纪 50 年代末期出现到 20 世纪 70 年代被广泛应用。

(4) 计算机密码。以计算机软件编程进行算法加密为特点,适用于计算机数据保护和网络通信等广泛用途的密码。

2. 按保密程度划分

(1) 理论上保密的密码。不管获取多少密文和有多大的计算能力,对明文始终不能得到唯一解的密码,称为理论上保密的密码,也称理论不可破的密码。如客观随机一次一密的密码就属于这种类型。

(2) 实际上保密的密码。在理论上可破,但在现有客观条件下,无法通过计算来确定唯一解的密码,称作实际上保密的密码。

(3) 不保密的密码。在获取一定数量的密文后可以得到唯一解的密码,叫作不保密密码。如早期的单表代替密码,后来的多表代替密码,以及明文加少量密钥等密码,现在都成为不保密的密码。

3. 按密钥方式划分

(1) 对称式密码。收发双方使用相同密钥的密码,称作对称式密码。传统的密码都属此类。

(2) 非对称式密码。收发双方使用不同密钥的密码,称作非对称式密码。如现代密码中的公共密钥密码就属此类。

4. 按明文形态划分

(1) 模拟型密码。用以加密模拟信息,如对动态范围之内,连续变化的语音信号加密的密码,称作模拟式密码。

(2) 数字型密码。用于加密数字信息,对两个离散电平构成 0、1 二进制关系的电报信息加密的密码称作数字型密码。

5. 按编制原理划分

可分为移位、代替和置换三种以及它们的组合形式。古今中外的密码,不论其形态多么繁杂,变化多么巧妙,都是按照这三种基本原理编制出来的。移位、代替和置换这三种原理在密码编制和使用中相互结合,灵活应用,形成了各种不同的密码算法。

3.2 常用加密技术

加密技术是对信息进行编码和解码的技术,编码是把原来可读信息(又称明文)译成代码形式(又称密文),其逆过程就是解码(解密)。常用加密技术主要分为对称加密算法和非对称加密算法。

3.2.1 对称加密算法

对称加密算法(Symmetric Algorithm)也称为传统密码算法,指加密和解密使用相同密钥的加密算法,就是加密密钥能够从解密密钥中推算出来,同时解密密钥也可以从加密密钥中推算出来。而在大多数的对称算法中,加密密钥和解密密钥是相同的,所以也称这种加密算法为秘密密钥算法或单密密钥算法。对称算法的安全性依赖于密钥的保密,泄漏密钥就意味着任何人都可以对他们发送或接收的消息解密,所以密钥的保密性对通信性至关重要。此外,每对用户每次使用对称加密算法时,都需要使用其他人不知道的唯一密钥,这会使得发信双发所拥有的密钥数量成几何级数增长,密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难,主要是因为密钥管理困难,使用成本较高。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA 和 AES。

1. DES 算法

美国国家标准局(NBS)于 1977 年公布了由 IBM 公司研制的一种加密算法,并批准把它作为非机要部门使用的数据加密标准(Data Encryption Standard,DES)。自从公布以来,它一直超越国界成为国际上商用保密通信和计算机通信的最常用的加密算法。当时规定 DES 的使用期为 10 年。后来美国政府宣布延长它的使用期,其原因大概有两条:一是 DES 尚未受到严重的威胁;二是一直没有新的数据加密标准问世。DES 超期服役了很长时间,在国际通信保密的舞台上活跃了 20 年。

DES 是 1972 年美国 IBM 公司研制的对称密码体制加密算法。明文按 64 位进行分组,密钥长 64 位,密钥事实上是 56 位参与 DES 运算(第 8、16、24、32、40、48、56、64 位是校验位,使得每个密钥都有奇数个 1)分组后的明文组和 56 位的密钥按位替代或交换的方法形成密文组的加密方法。

1) DES 工作的基本原理

入口参数有三个:key、data、mode。key 为加密解密使用的密钥,data 为加密解密的数据,mode 为其工作模式。当模式为加密模式时,明文按照 64 位进行分组,形成明文组,key 用于对数据加密,当模式为解密模式时,key 用于对数据解密。实际运用中,密钥只用到了 64 位中的 56 位,这样才具有高的安全性。DES 工作的基本原理如图 3-3 所示。

明文
初始置换
16轮运算
末置换
密文

图 3-3 DES 基本原理

2) DES 算法的主要流程

DES 算法把 64 位的明文输入块变为 64 位的密文输出块,它所使用的密钥也是 64 位。整个算法的主流程如图 3-4 所示。DES 算法大致可以分成四个部分:初始置换、迭代过程和逆置换,迭代过程中又涉及置换表、函数 f、S 盒以及子密钥生成等。

(1) 置换规则表。

初始置换和逆置换均是按照一张置换表的置换规则进行置换。初始置换主要有输入的 64 位数据按 IP 置换表进行重新组合,并把输出分为 L_0、R_0 两部分,每部分各长 32 位,其 IP

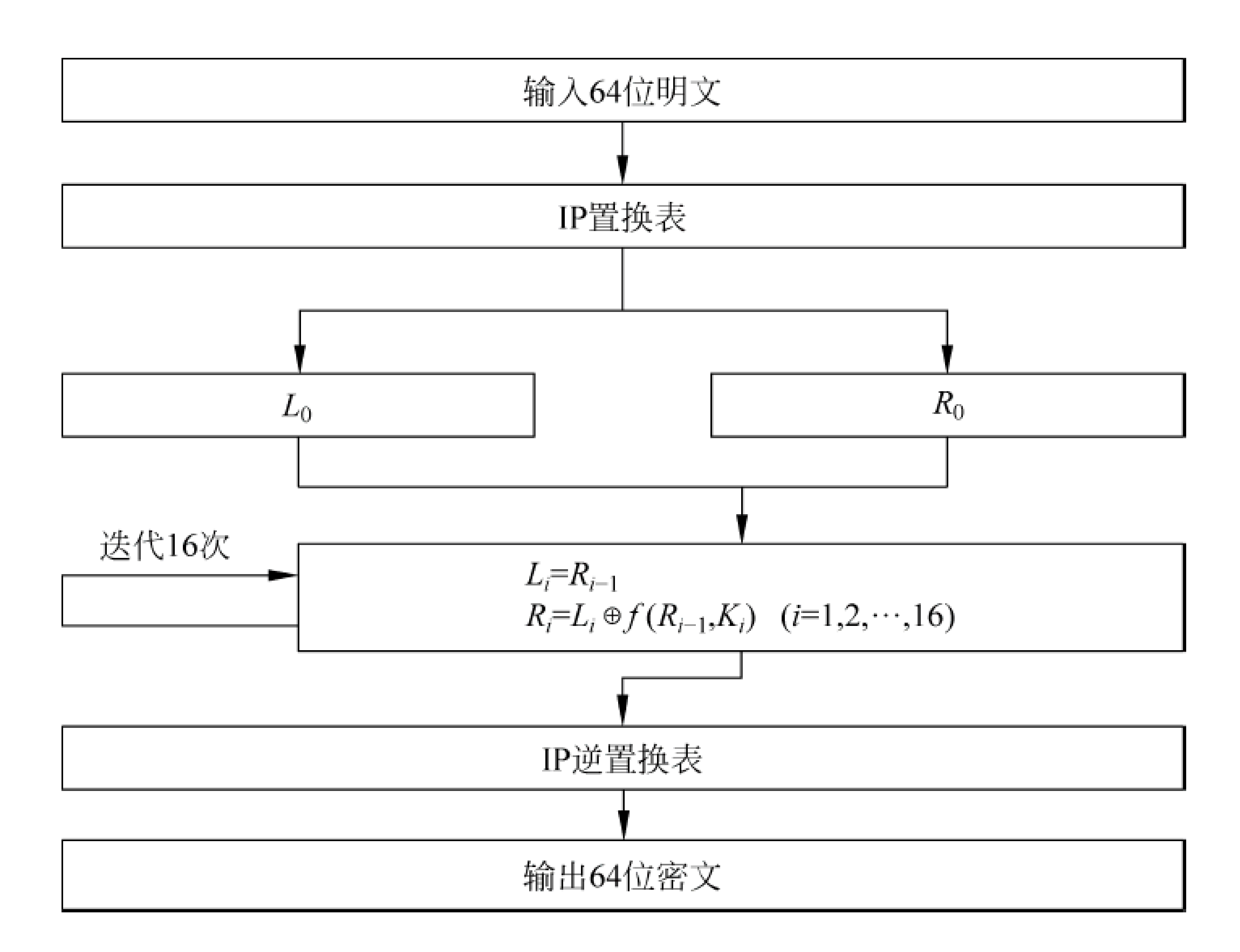


图 3-4　DES 算法流程图

置换表如表 3-1 所示。

表 3-1　IP 置换表

58	50	12	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

即将输入的 58 位换到第 1 位，第 50 位换到第 2 位，以此类推，最后一位是原来的第 7 位。L_0、R_0 则是换位输出后的两部分，L_0 是输出的左 32 位，R_0 是右 32 位。例如，设置换前的输入值为 $D_1D_2D_3\cdots D_{64}$，则经过初始置换后的结果为 $L_0=D_{58}D_{50}\cdots D_8$；$R_0=D_{57}D_{49}\cdots D_7$。

经过 16 次迭代运算后，得到 L_{16}、R_{16}，将此作为输入，进行逆置换，即得到密文输出。逆置换正好是初始置换的逆运算。例如，第 1 位经过初始置换后，处于第 40 位，而通过逆置换 IP-1，又将第 40 位换回到第 1 位，其逆置换 IP-1 规则如表 3-2 所示。

表 3-2　IP-1 逆置换表

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

（2）迭代过程。

在 16 轮迭代的过程中，将每轮 64 比特的输入分成 32 比特的左右两半，分别记为 L 和

R,每轮变换可用下列公式表示:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

如上述公式所示,第 i 轮迭代的左半部分直接即为第 $i-1$ 轮的右半部分,而第 i 轮右半部分为第 $i-1$ 轮左半部分异或 $f(R_{i-1}, K_i)$。

(3) 函数 f。

函数 f 有两个输入:32 位的 R_{i-1} 和 48 位 K_i,f 函数的处理流程如图 3-5 所示。

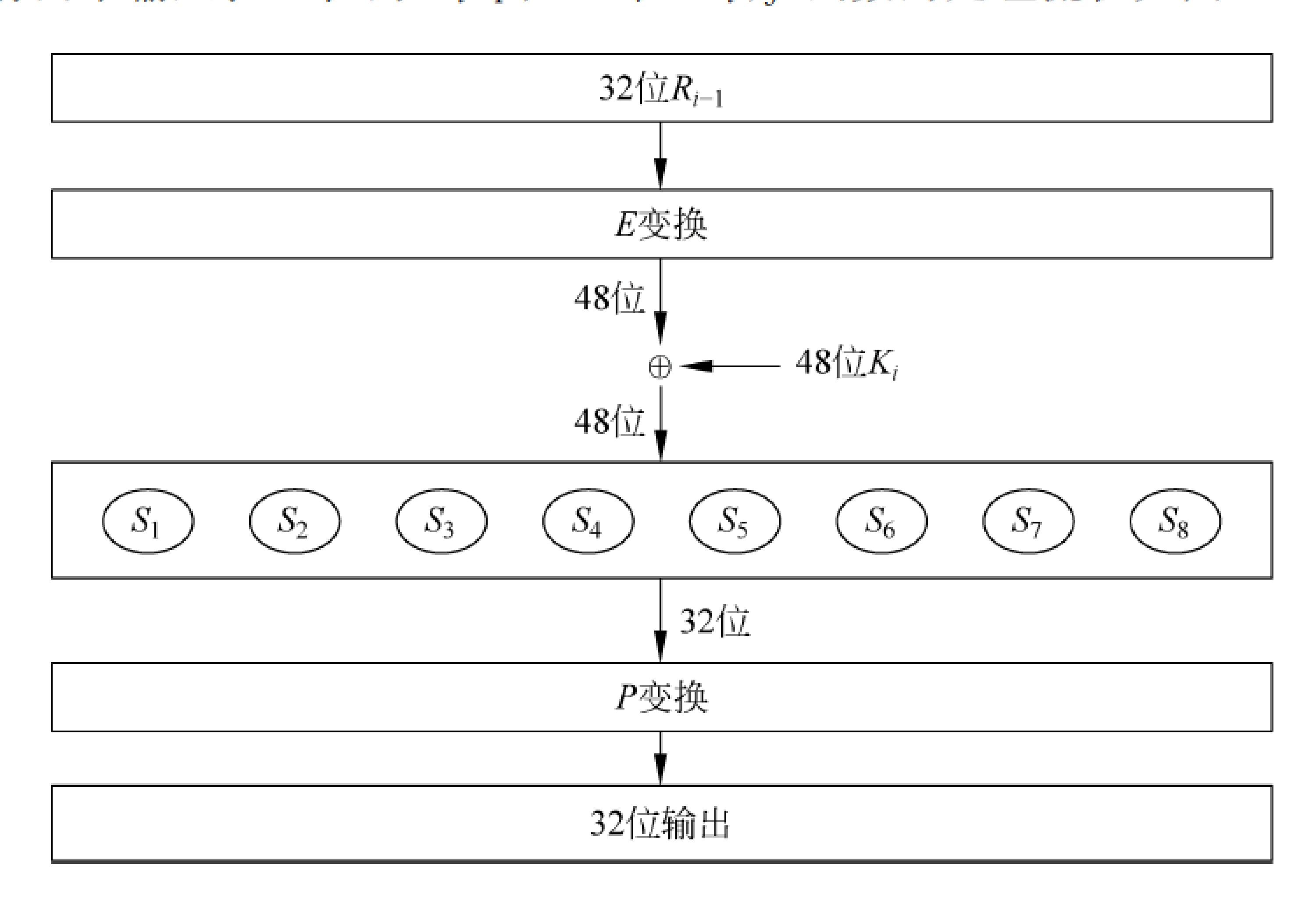


图 3-5　f 函数的处理流程图

(4) 换位表。

图 3-5 中 E 变换的算法是从 R_{i-1} 的 32 位中选取某些位,构成 48 位。即 E 将 32 比特扩展变换为 48 位,变换规则根据 E 置换表,如表 3-3 所示。

表 3-3　E 置换表

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

图 3-5 中 P 变换的算法是从 S 盒的输出作为 P 变换的输入,P 的功能是对输入进行置换,P 置换表如表 3-4 所示。

表 3-4　P 置换表

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

(5) 子密钥 K_i。

假设密钥为 K,长度为 64 位,但是其中第 8、16、24、32、40、48、64 用作奇偶校验位,实际上密钥长度为 56 位。K 的下标 i 的取值范围是 1～16,用 16 轮变换来构造。

子密钥 K_i 的构造过程如图 3-6 所示。

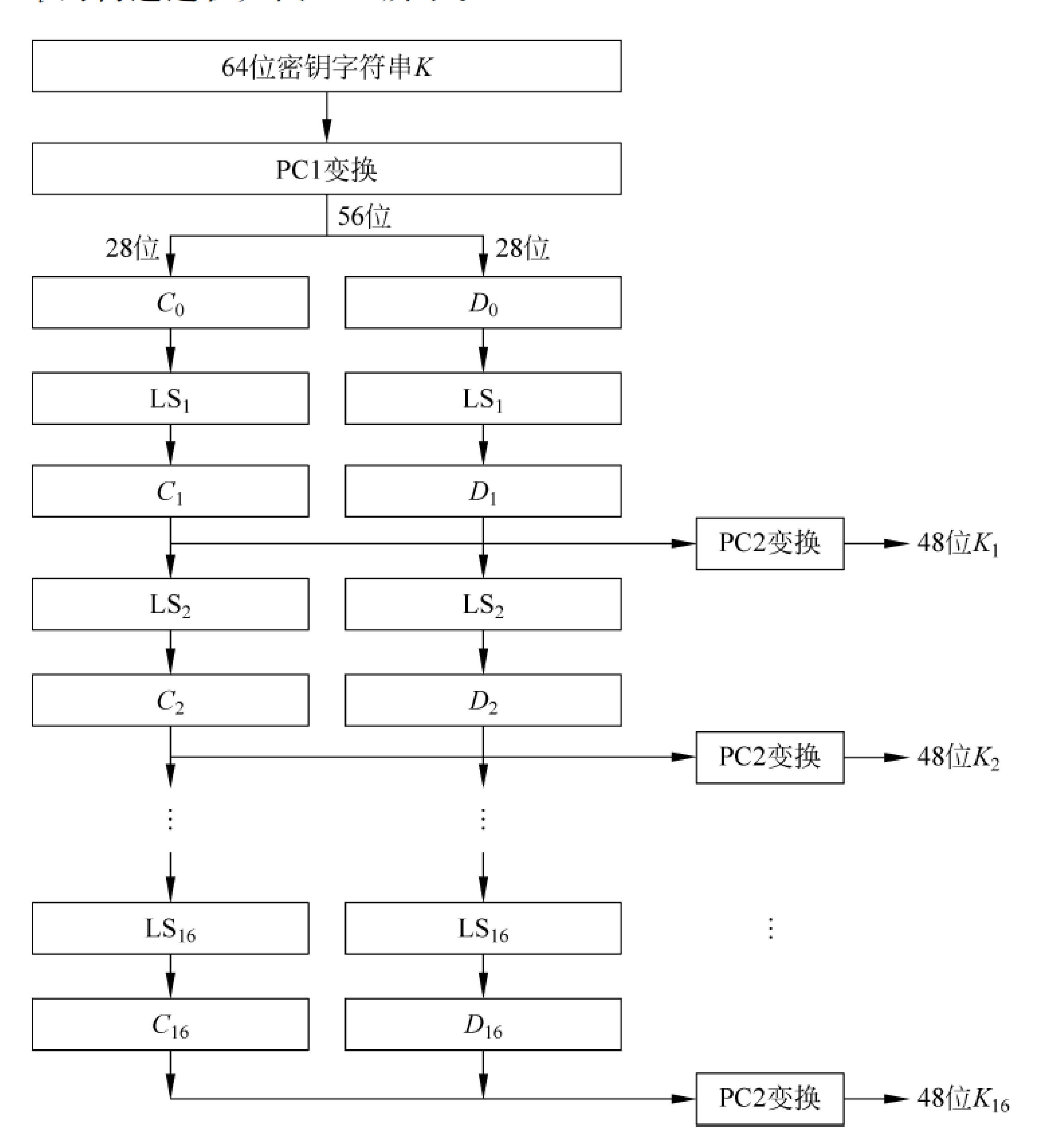


图 3-6　子密钥 K_i 生成过程

首先，对于给定的密钥 K，应用 PC1 变换进行选位，选定后的结果是 56 位，设其前 28 位为 C_0，后 28 位为 D_0。PC1 选位如表 3-5 所示。

表 3-5　PC1 变换表

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

第一轮：对 C_0 作左移 LS1 得到 C_1，对 D_0 作左移 LS1 得到 D_1，对 C_1D_1 应用 PC2 进行选位，得到 K_1。其中 LS1 是左移的位数，如表 3-6 所示。

表 3-6　LS 左移表

1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 3-6 中的第一列是 LS1，第二列是 LS2，以此类推。左移的原理是所有二进位向左移

动，原来最右边的比特位移动到最左边。其中 PC2 如表 3-7 所示。

表 3-7　PC2 变换表

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

第二轮：对 C_1、D_1 作左移 LS2 得到 C_2 和 D_2，进一步对 C_2、D_2 应用 PC2 进行选位，得到 K_2。如此继续，分别得到 K_3，K_4，…，K_{16}。

(6) *S* 盒的工作原理。

S 盒以 6 位作为输入，而以 4 位作为输出，现在以 S_1 为例说明其过程。假设输入为 $A=a1a2a3a4a5a6$，则 $a2a3a4a5$ 所代表的数是 0～15 之间的一个数，记为：$k=a2a3a4a5$；由 $a1a6$ 所代表的数是 0～3 间的一个数，记为 $h=a1a6$。在 S_1 的 h 行，k 列找到一个数 B，B 在 0～15 之间，它可以用 4 位二进制表示，为 $B=b1b2b3b4$，这就是 S_1 的输出，如图 3-7 所示。

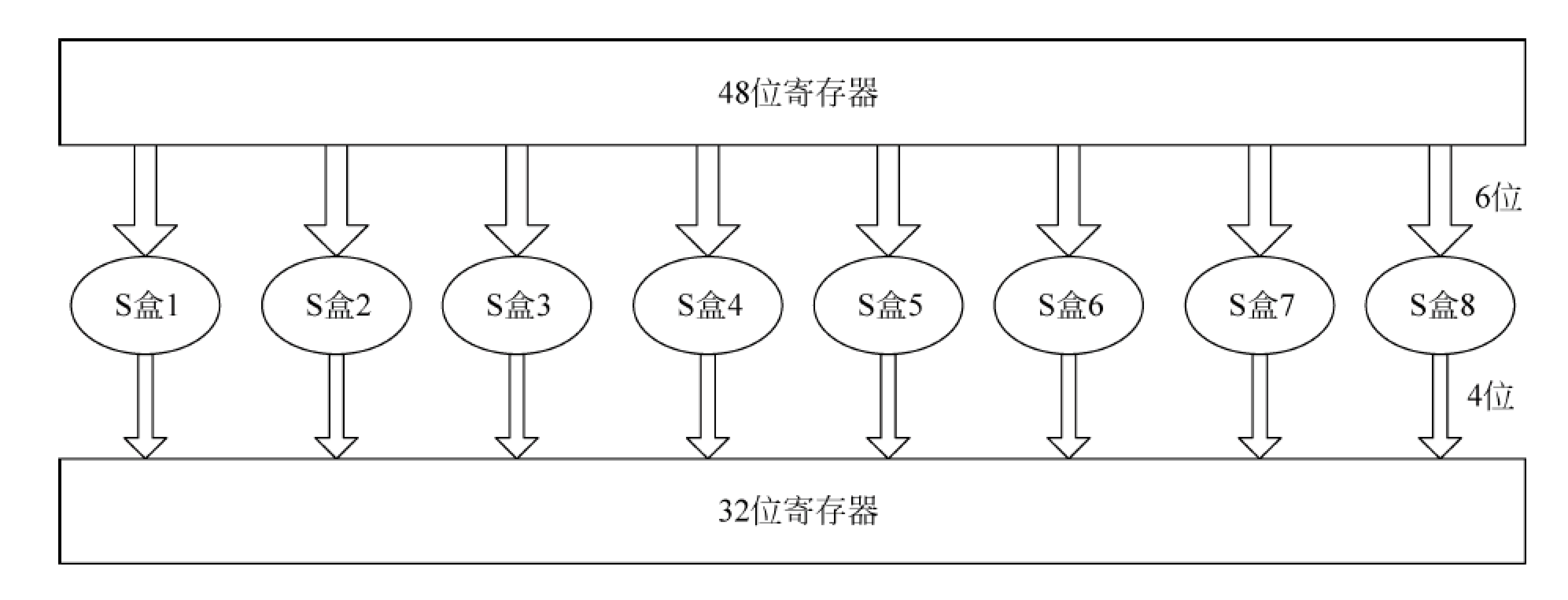


图 3-7　*S* 盒变换

如 6 位输入的第 1 和第 6 位组合构成了 2 位二进制数，可表示十进制数 0～3，它对应着表中的一行；6 位输入的第 2 到第 5 位组合构成了 4 位二进制数，可表示十进制数 0～15，它对应着表中的一列。假设 S_1 盒的 6 位输入是 110100，其第 1 位和第 6 位组合为 10，它对应 S_1 盒的第 2 行；中间 4 位组合为 1010，它对应 S_1 盒的第 10 列。S_1 盒的第 2 行第 10 列的数是 9，其二进制数为 1001(行和列的计数均从 0 开始而非从 1 开始)。1001 即为输出，则 1001 就代替了 110100。

DES 算法的解密过程是一样的，区别仅仅在于第一次迭代时用子密钥 K_{15}，第二次 K_{14}，最后一次用 K_0，算法本身并没有任何变化。DES 的算法是对称的，既可用于加密又可用于解密。

3) DES 算法的安全性

DES 算法是安全性比较高的一种算法，目前只有一种方法可以破解该算法，那就是穷举法。采用 64 位密钥技术，实际只有 56 位有效，8 位用来校验。譬如，有这样的一台 PC，

它能每秒计算一百万次，那么对于 256 位空间，要穷举它的时间为 2285 年，所以这种算法还是比较安全的一种算法。

2. 三重 DES(3DES)

DES 的主要密码学缺点就是密钥长度较短。为了解决使用 DES 技术 56 位时密钥日益减弱的强度问题，其办法之一是采用三重 DES 算法(Triple DES 或 3DES)，即使用两个独立密钥 K_1 和 K_2 对明文运行 DES 算法三次，得到 112 位有效密钥强度，若对 3DES 的穷举攻击需要 2112 次，而不是 DES 的 264 次。其算法的步骤如下：

(1) 用密钥 K_1 进行 DES 加密；

(2) 用步骤(1)的结果使用密钥 K_2 进行 DES 解密；

(3) 用步骤(2)的结果使用密钥 K_1 进行 DES 加密。

这个过程称为 EDE，因为它是由加密-解密-加密(Encrypt Decrypt Encrypt)步骤组成的。在 EDE 中，中间步骤是解密，所以，可以使 $K_1=K_2$ 来用三重 DES 方法执行常规的 DES 加密。

三重 DES 的缺点是时间开销较大，三重 DES 的时间是 DES 算法的 3 倍。但从另一方面看，三重 DES 的 112 位密钥长度在可以预见的将来可认为是适合的。

DES 被认为是安全的，这是因为要破译它可能需要尝试 256 位密钥直到找到正确的密钥。

3. IDEA 加密

1) IDEA 加密算法概述

国际数据加密算法(International Data Encryption Algorithm，IDEA)是瑞士的 James Massey、Xuejia Lai 等人提出的加密算法，在密码学中属于数据块加密算法(Block Cipher)类。IDEA 使用长度为 128 位的密钥，数据块大小为 64 位。从理论上讲，IDEA 属于“强”加密算法，至今还没有出现对该算法的有效攻击算法。

早在 1990 年，Xuejia Lai 等人在 EuroCrypt’90 年会上提出了分组密码建议(Proposed Encryption Standard，PES)。在 EuroCrypt’91 年会上，Xuejia Lai 等人又提出了 PES 的修正版 IPES(Improved PES)。目前 IPES 已经商品化，并改名为 IDEA。IDEA 已由瑞士的 Ascom 公司注册专利，以商业目的使用 IDEA 算法必须向公司申请许可。

这种算法是在 DES 算法的基础上发展出来的，类似三重 DES。发展 IDEA 也是因为感到 DES 具有密钥太短等缺点，已经过时。IDEA 的密钥为 128 位，这么长的密钥在今后若干年内应该是安全的。类似于 DES，IDEA 算法也是一种数据块加密算法，它设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。与 DES 的不同处在于，它采用软件实现和采用硬件实现同样快速。由于 IDEA 是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制，因此，有关 IDEA 算法和实现技术的书籍都可以自由出版和交流，可极大地促进 IDEA 的发展和完善。

目前 IDEA 在工程中已有大量应用实例，PGP(Pretty Good Privacy)就使用 IDEA 作为其分组加密算法；安全套接字(Secure Socket Layer，SSL)也将 IDEA 包含在其加密算法库 SSLRef 中；IDEA 算法专利的所有者 Ascom 公司也推出了一系列基于 IDEA 算法的安全

产品，包括基于 IDEA 的 Exchange 安全插件、IDEA 加密芯片、IDEA 加密软件包等。IDEA 算法的应用和研究正在不断走向成熟。

2）IDEA 算法原理

IDEA 是一种由 8 个相似圈(Round)和一个输出变换(Output Transformation)组成的迭代算法。IDEA 的每个圈都包含三种基本运算，即乘法、加法和异或。在加密之前，IDEA 通过密钥扩展(Key Expansion)将 128bit 的密钥扩展为 52Byte 的加密密钥(Encryption Key，EK)，然后由 EK 计算出解密密钥(Decryption Key，DK)。EK 和 DK 分为 8 组半密钥，每组长度为 6Byte，前 8 组密钥用于 8 圈加密，最后半组密钥(4Byte)用于输出变换。IDEA 的加密过程和解密过程是一样的，只不过使用不同的密钥(加密时用 EK，解密时用 DK)。

密钥扩展的过程如下：

（1）将 128bit 的密钥作为 EK 的前 8byte；

（2）将前 8byte 循环左移 25bit，得到下一 8byte，将这个过程循环 7 次；

（3）在第 7 次循环时，取前 4byte 作为 EK 的最后 4byte；

（4）至此 52byte 的 EK 生成完毕。

3）IDEA 算法的安全性

IDEA 算法的密钥为 128bits(DES 的密钥为 56bits)，设计者尽最大努力使该算法不受差分密码分析的影响，数学家已证明 IDEA 算法在其 8 圈迭代的第 4 圈之后便不受差分密码分析的影响了。假定穷举法攻击有效的话，那么即使设计一种每秒钟可以试验 10 亿个密钥的专用芯片，并将 10 亿片这样的芯片用于此项工作，仍需 1013 年才能解决问题；另一方面，若用 1024 片这样的芯片，有可能在一天内找到密钥，不过人们还无法找到足够的半导体材料来设计和制造这样的芯片。目前，尚无一篇公开发表的试图对 IDEA 进行密码分析的文章。因此，就现在来看应当说 IDEA 是非常安全的。并且，IDEA 算法比 RSA 算法快得多，又比 DES 算法要相对安全得多。

3.2.2 非对称加密算法

美国斯坦福大学的两名学者 W. Diffie 和 M. Hellman 于 1976 年在 IEEE Transactions on Information Theory 杂志上发表了文章 New Direction in Cryptography，提出了“公开密钥密码体制”的概念，开创了密码学研究的新方向。公开密钥密钥体制的产生主要有两个方面的原因：一是由于对称密钥密码体制的密钥分配问题，二是由于对数字签名的需求。

非对称密码系统的解密密钥与加密密钥是不同的，一个称为公开密钥，另一个称为私人密钥(或秘密密钥)，因此这种密码体系也称为公钥密码体系。公钥密码体制的算法中最著名的代表是 RSA 算法，此外还有椭圆曲线、背包密码、McEliece 密码、Diffe-Hellman、Rabin 和 ElGamal 算法等。

1. RSA 算法

RSA 算法是最著名、应用最广的公钥密码算法。它是在 1978 年由 Rivest、Shamir 和 Adleman 三个人共同提出的，并以三个发明者的名字的首字母命名。RSA 的安全性取决于大模数的因子分解的困难性，其公开密钥和私人密钥是一对大素数(100 到 200 位的十进制

数或更大)的函数,从一个公开密钥和密文中恢复出明文的难度等同于分解两个大素数之积的难度。从严格的技术角度上来说这是不正确的,在数学上至今还没有证明分解模数就是攻击 RSA 的最佳方法,也未能证明分解大整数就是 NP 问题。事实的情况是,大整数因子分解问题过去几百年来一直是令数学家头疼而又未能有效解决的世界性难题。人们设想了一些非因子分解的途径来攻击 RSA 算法,但这些方法都不比分解模数来得容易。因此,严格地说,RSA 的安全性基于求解其单向函数的逆的困难性。RSA 单向函数求逆的安全性没有真正的因子分解模数的安全性高,而且目前人们也无法证明这两者是等价的。许多研究人员都试图改进 RSA 算法使它的安全性等价于因子分解模数。

RSA 是最具代表性的公钥密码算法,可能也是最知名和最古老的公钥密码算法。由于算法完善(既可以用于数据加密,又可用于数字签名),安全性良好,易于理解和实现,RSA 已经成为了一种应用极为广泛的公钥密码算法。

RSA 算法的思路如下:

1) 密钥生成

(1) 系统产生两个大素数 p,q(保密)。为了获得最大程度的安全性,选两数的长度一样。

(2) 计算模数 $n=p\times q$(公开),欧拉函数 $\Phi(n)=(p-1)\times(q-1)$(保密)。

(3) 随机选取加密密钥 e,使 e 和 $\Phi(n)$互素,即满足:$0<e<\Phi(n)$ 且 $\gcd(e,\Phi(n))=1$。

(4) 用欧几里得(Euclidean)扩展算法计算解密密钥 d,d 满足 $e\times d\equiv 1 \bmod \Phi(n)$,即 $d=e-1 \bmod \Phi(n)$。

(5) e 和 n 为公开密钥,d 是私人密钥。两个大数 p 和 q 应该立即丢弃,不让任何人知道。一般选择公开密钥 e 比私人密钥 d 小。最常选用的 e 值有 3 个,即 3、17、65 537。

2) RSA 加密和解密过程

加密消息时,首先将明文分组并数字化,每个数字化分组明文的长度不大于 n(采用二进制数,选到小于 n 的 $2d$ 的最大次幂),设 mi 表示消息分组,ci 表示加密后的密文,它与 mi 具有相同的长度。

对每个明文分组 m 依次进行加解密运算:

(1) 加密运算:使用公钥 e 和要加密的明文 m 进行 ci=mie(mod n)运算即得密文。

(2) 解密运算:使用私钥 d 和要解密的密文 c 进行 mi=ci$d$(mod n)运算即得明文。RSA 的实现过程如图 3-8 所示。

下面举例说明 RSA 算法的实现过程。

① 取两个质数 $p=11$,$q=13$,p 和 q 的乘积为 $n=p\times q=143$;

② 算出另一个数 $\Phi(n)=(p-1)\times(q-1)=120$;

③ 再选取一个与 $\Phi(n)=120$ 互质的数,例如 $e=7$,则公开密钥$=(n,e)=(143,7)$;

④ 对于这个 e 值,可以算出其逆:$d=103$。因为 $e\times d=7\times 103=721$,满足 $e\times d \bmod \Phi(n)=1$;即 $721 \bmod 120=1$ 成立,则秘密密钥$=(n,d)=(143,103)$。

设张小姐需要发送机密信息(明文)$m=85$ 给李先生,她已经从公开媒体得到了李先生的公开密钥$(n,e)=(143,7)$,于是她算出加密值:$c=me \bmod n=857 \bmod 143=123$ 并发送给李先生。

李先生在收到密文 $c=123$ 后,利用只有他自己知道的秘密密钥计算:$m=cd \bmod n=$

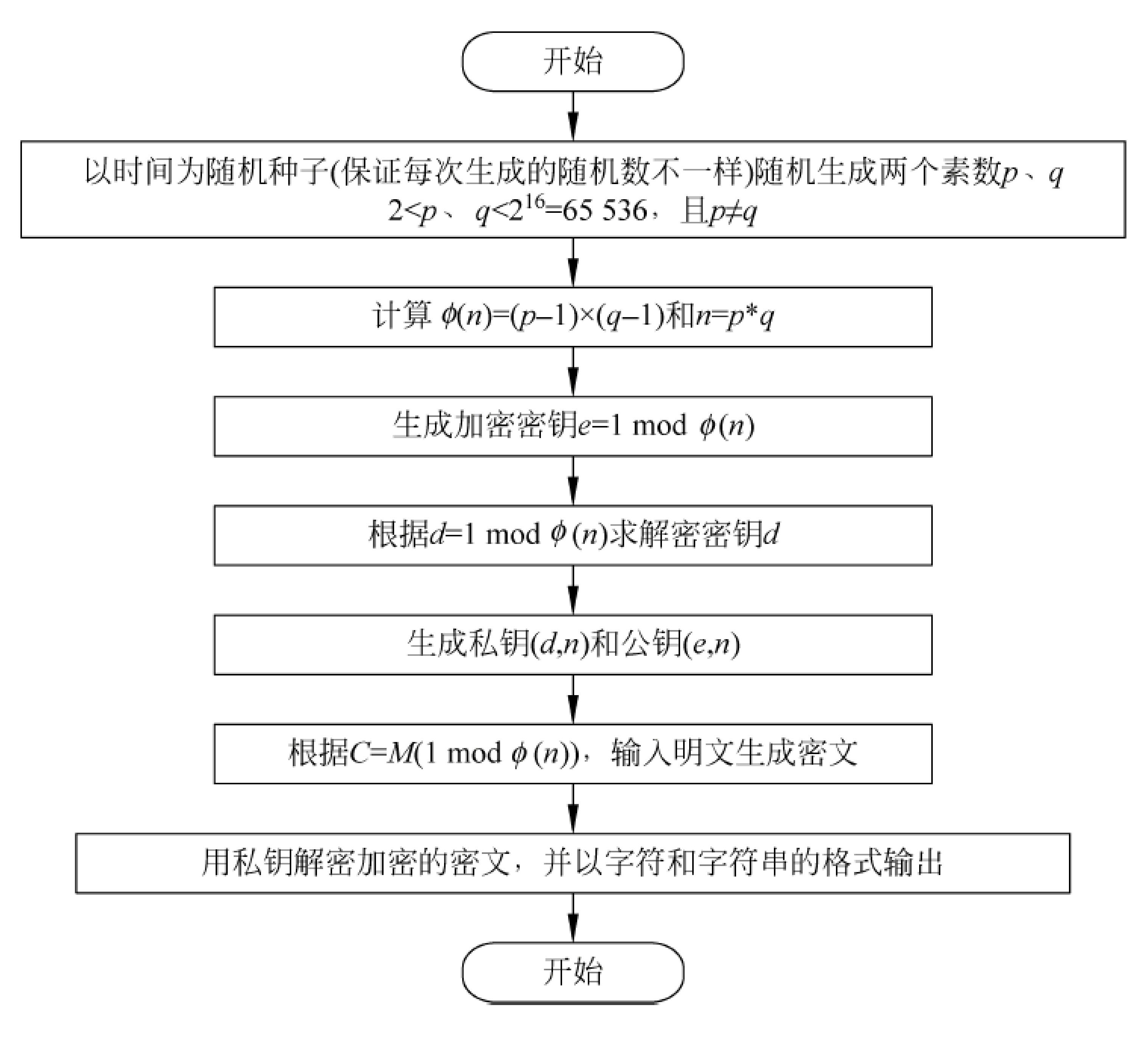


图 3-8 RSA 算法的实现过程

123103 mod 143＝85,所以,李先生可以得到张小姐发给他的真正的信息 $m=85$,实现了解密。

3）RSA 算法的特点及应用

RSA 算法具有密钥管理简单(网上每个用户仅需保密一个密钥,且不需配送密钥)、便于数字签名、可靠性较高(取决于分解大素数的难易程度)等优点,但也具有算法复杂、加密/解密速度慢、难于用硬件实现等缺点。因此,公钥密码体制通常被用来加密关键性的、核心的、少量的机密信息,而对于大量要加密的数据通常采用对称密码体制。

RSA 算法的安全性建立在难于对大整数提取因子的基础上,已知的证据都表明大整数因式分解问题是一个极其困难的问题。但是,随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展,要求作为 RSA 加密/解密安全保障的大整数越来越大。

RSA 算法的保密性,取决于 dui 大素数因式分解的时间。假定用 106 次/秒的计算机进行运算,用最快的公式分解 $n=100$ 位十进制数要用 74 年,分解 200 位数要用 3.8×109 年。可见,当 n 足够大时(p 和 q 各为 100 位时,n 为 200 位),对其进行分解是很困难的。可以说,RSA 的保密强度等价于分解 n 的难易程度。

RSA 算法为公用网络上信息的加密和鉴别提供了一种基本的方法。他通常是先生成一对 RSA 密钥,其中之一是保密密钥,由用户保存;另一个为公开密钥,可对外公开,甚至可在网络服务器中注册。

2. 椭圆曲线密码算法

1）椭圆曲线密码概述

椭圆曲线密码学(Elliptic Curve Cryptography,ECC)是基于椭圆曲线数学的一种公钥

密码的方法。椭圆曲线在密码学中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的。ECC 的主要优势是在某些情况下它比其他的方法使用更小的密钥(如 RSA)提供相当的或更高等级的安全。ECC 的另一个优势是可以定义群之间的双线性映射,基于 Weil 对或 Tate 对。双线性映射已经在密码学中发现了大量的应用,例如基于身份的加密。不过它的一个缺点是加密和解密操作的实现比其他机制花费的时间长。椭圆曲线密码学的许多形式稍微有所不同,所有的都依赖于被广泛承认的解决椭圆曲线离散对数问题的困难性上,对应有限域上椭圆曲线的群。

椭圆曲线是用三次方程来表示的,该方程与计算椭圆周长的方程相似,因而称为椭圆曲线。在 ECC 中,我们关心的是某种特殊形式的椭圆曲线,即定义在有限域上的椭圆曲线,椭圆曲线的吸引人之处在于提供了由"元素"和"组合规则"来组成群的构造方式,用这些群来构造密码算法具有完全相似的特性,且没有减少密码分析的分析量。

2）椭圆曲线国际标准

椭圆曲线密码系统已经形成了若干国际标准,其涉及加密、签名、密钥管理等方面,包括:

(1) IEEE P1363:加密、签名、密钥协商机制。

(2) ANSI X9:椭圆曲线数字签名算法,即椭圆曲线密钥协商和传输协议。

(3) ISO/IEC:椭圆曲线 ElGamal 体制签名。

(4) IETF:椭圆曲线 DH 密钥交换协议。

(5) ATM Forum:异步传输安全机制。

(6) FIPS 186-2:美国政府用于保证其电子商务活动中的机密性和完整性。

3）椭圆曲线技术实现

ECC 的技术实现可以分成 4 个层次:运算层、密码层、接口层和应用层。运算层最基础、最核心;应用层最接近用户。

(1) 运算层。

运算层的主要功能是提供密码算法的所有数论运算支持,包括大整数加、减、乘、除、模、逆、模幂等。运算层的实现效率将对整个密码系统的效率起决定性作用。因而运算层的编程工作是算法实现最核心、最基础,也是最艰巨的部分。

(2) 密码层。

密码层的主要功能是在运算层的支持上选择适当的密码体制,科学地、准确地、安全地实现密码算法。在相同的运算层的基础上,可以构建起多种密码体制。对于密码体制和具体结构的选择和实现是密码层的核心内容。最终,密码系统的安全性将决定于密码层的实现能力。在密码层中,为了支持公钥密码系统,通常必须提供 5 种操作,即生成密钥对、加密、解密、签名和验证签名。

(3) 接口层。

接口层的主要功能是对各种软硬件平台提供公钥密码功能支持。其工作重点在于对各种硬件环境的兼容、对各种操作系统的兼容、对各种高级语言的兼容、对多种应用需求兼容。其难点主要在于保持良好的一致性、可移植性、可重用性,以有限的资源换取应用层尽可能多的自由空间。

(4) 应用层。

应用层是最终用户所能接触到的唯一层面,它为用户提供应用功能和操作界面。应用功能包括交易、网络、文件、数据库、加解密、签名及验证等。操作界面包括图形、声音、指纹、键盘、鼠标等。

ECC 的实现效率一般表现为 ECC 公钥密码功能的效率。实现效率是被多种因素制约和影响的。下面列举了在实现 ECC 公钥密码功能效率。实现效率是被多种因素制约和影响的。下面列举了在实现 ECC 的过程中遇到的涉及 ECC 实现效率的方面。

① ECC 密码机制。众所周知,任何密码理论都必须在某种密码机制上实现才能完成密码功能(如加密、签名等)。同一种密码理论也可以运用于不同的密码机制上,而且它们的实现效率也不尽相同。我们在自行发明的、拥有自主知识产权的密码机制上实现 ECC,并且容易证明其安全性不低于其他常用密码体制,且效率更高。

② 安全前瞻性。由于公钥系统的安全性建立在数学的困难性上,因此在选择 ECC 参数时,不能一味地追求速度快,而是应该在理论上、实现上都要为安全性留出一定的余量,以保证在密码分析技术进步后,不致受到重大威胁。ECC 安全性的保障是要通过降低一定的效率来换取的。

③ 应用环境。应用环境是 ECC 软硬件实现的约束条件。硬件环境要求空间小、指令简单、高稳定性、低成本;软件环境要求兼容性好、可移植性好、易于维护升级。因此,从高端到低端,从高级语言到汇编、从系统到门电路设计,每个应用环境对 ECC 实现所提供的支持和约束都不相同。所以,ECC 实现效率也依应用环境而异。

④ 算法优化。算法优化始终都是提高效率的根本所在。对 ECC 实现算法的优化主要从这几个方面入手:对数学公式的变形和组合优化;在软件实现中,根据编译系统的特点、CPU 指令集的特点优化;在硬件实现中,根据硬件资源的具体特点优化。

3.3 密码技术的应用

网络安全系统的一个很重要方面是防止非法用户对系统的主动攻击,如伪造信息、篡改信息等。这种安全要求对实际网络系统的应用(如电子商务)是非常重要的。以下介绍的鉴别、数字签名、物联网认证与访问控制以及公钥基础设施等都是基于数据加密的应用技术。

3.3.1 鉴别技术

1. 基本概念

鉴别(authentication,也叫验证)是防止主动攻击的重要技术。鉴别的目的就是验证用户身份的合法性和用户间传输信息的完整性与真实性。

鉴别服务主要包括信息鉴别和身份验证两方面。信息鉴别和身份验证可采用数据加密技术、数字签名技术及其他相关技术来实现。

信息鉴别是为了确保数据的完整性和真实性,对信息的来源、时间性及目的地进行验证。信息鉴别过程通常涉及加密和密钥交换。加密可使用对称密钥加密、非对称密钥加密或两种加密方式的混合。信息经验证后表明,它在发送期间没有经过篡改,发送者经验证后

表明，他就是合法的发送者。

身份验证是验证进入网络系统者是否是合法用户，以防非法用户访问系统。身份验证的方式一般有用户口令验证、摘要算法验证、基于 PKI(公钥基础设施)的验证等。验证、授权和访问控制都与网络实体安全有关。

网络中的通信除需要进行消息的验证外，还需要建立一些规范的协议对数据来源的可靠性、通信实体的真实性加以认证，以防止欺骗、伪装等攻击。例如：A 和 B 是网络的两个用户，他们想通过网络先建立安全的共享密钥再进行保密通信，那么 A 如何确信自己正在和 B 通信而不是和 C 通信呢？这种通信方式为双向通信，因此此时的认证称为互相认证。类似地，对于单向通信来说，认证称为单向认证。

认证中心(Certificate Authority，CA)在网络通信认证技术中具有特殊的地位。例如，电子商务，认证中心是为了从根本上保障电子商务交易活动顺利进行而设立的，主要是解决电子商务活动中参与各方的身份、资信的认定，维护交易活动的安全。CA 是提供身份验证的第三方机构，通常由一个或多个用户信任的组织实体组成。例如，持卡人(客户)要与商家通信，持卡人从公开媒体上获得了商家的公开密钥，但无法确定商家不是冒充的(有信誉)，于是请求 CA 对商家认证。此时，CA 对商家进行调查、验证和鉴别后，将包含商家公钥的证书传给持卡人。同样，商家也可对持卡人进行验证，其过程为持卡人→商家；持卡人→CA；CA→商家。证书一般包含拥有者的标识名称和公钥，并且由 CA 进行数字签名。CA 的功能主要包括接收注册申请、处理、批准/拒绝请求和颁发证书。

在实际运作中，CA 也可由大家都信任的一方担当，例如，在客户、商家、银行三角关系中，客户使用的是由某个银行发的卡，而商家又与此银行有业务关系(有账号)。在此情况下，客户和商家都信任该银行，可由该银行担当 CA 角色，接受和处理客户证书和商家证书的验证请求。又如，对商家自己发行的购物卡，则可由商家自己担当 CA 角色。

2. 信息的验证

从概念上说，信息的签名就是用专用密钥对信息进行加密，而签名的验证就是用相对应的公用密钥对信息进行解密。但是，完全按照这种方式行事也有缺点。因为，同普通密钥系统相比，公用密钥系统的速度很慢，用公用密钥系统对长信息加密来达到签名的目的，并不比用公用密钥系统来达到信息保密的目的更有吸引力。

解决方案就是引入另一种普通密码机制，这种密码机制叫做信息摘要或散列函数。信息摘要算法从任意大小的信息中产生固定长度的摘要，而其特性是没有一种已知的方法能找到两个摘要相同的信息。这就意味着，虽然摘要一般要比信息小得多，但是可以在很多用途方面看作是与完整信息等同的。最常用的信息摘要算法叫做 MD5，可产生一个 128 位长的摘要。

使用信息摘要时，对信息签名的过程如下：

(1) 用户制作信息摘要。

(2) 信息摘要由发送者的专用密钥加密。

(3) 原始信息和加密信息摘要发送到目的地。

(4) 目的地接收信息，并使用与原始信息相同的信息摘要函数对信息制作其自己的信息摘要。

(5) 目的地对所收到的信息摘要进行解密。

(6) 目的地将制作的信息摘要同附有信息的信息摘要进行对比,如果相吻合,目的地就知道信息的文本与用户发送的信息文本是相同的,如果二者不吻合,则目的地知道原始信息已经被修改过。

这一过程还有另外一个长处,这个长处可取名为数字签名。由于只有用户知道私用密钥,因而只有用户能够制作加密的信息摘要。任何一个可以获取公用密钥的目的地都可弄清楚签名者的身份。这一技术可用于最流行的程序,用以保护包括 PGP 和 PEM(保密增强邮件)在内的电子邮件。

3. 身份验证

身份认证是在计算机网络中确认操作者身份的过程。身份认证可分为用户与主机间的认证和主机与主机之间的认证。用户与主机之间的认证可以基于如下一个或几个因素：用户所知道的东西,例如口令、密码等；用户拥有的东西,例如印章、智能卡(如信用卡等)；用户所具有的生物特征,例如指纹、声音、视网膜、签字和笔迹等。

计算机网络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的,计算机只能识别用户的数字身份,所有对用户的授权也是针对用户数字身份的授权。如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者,也就是说保证操作者的物理身份与数字身份相对应,身份认证就是为了解决这个问题。作为防护网络资产的第一道关口,身份认证有着举足轻重的作用。

在真实世界,对用户的身份认证基本方法可以分为三种：

(1) 根据你所知道的信息来证明你的身份(what you know,你知道什么)；

(2) 根据你所拥有的东西来证明你的身份(what you have,你有什么)；

(3) 直接根据独一无二的身份特征来证明你的身份(who you are,你是谁),如指纹、面貌等；

在网络世界中的手段与真实世界中一致,为了达到更高的身份认证安全性,某些场景会将上面三种认证方法中的两种混合使用,即所谓的双因素认证。

进入电子信息社会,虽然有不少学者试图使用电子化生物唯一识别信息,但是出于其代价高、准确性低、存储空间大和传输速率低,不适合计算机读取和判断,只能作为辅助措施应用。而使用密码技术,特别是公钥密码技术,能够设计出安全性高的识别协议,受到人们的青睐。

过去人们采用通行字作为用户身份识别,通行字短、固定、规律性强、易暴露、安全性差。现在采用密码技术进行交互式询答,只有拥有正确密码的合法用户才能通过询答。目前已经用于身份认证的 IC 卡、数字证书、一次性口令等,它们都采用了密码技术。

3.3.2 数字签名技术

1. 基本概念

数字签名,又称为公钥数字签名、电子签章,是只有信息的发送者才能产生的别人无法伪造的一段数字串,这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。

目前的数字签名大多是建立在公开密钥体制基础上的，这是公开密钥加密技术的另一种重要应用，如基于RSA的公开密钥加密标准PKCS、数字签名算法DSA、PGP加密软件等。1994年美国标准与技术协会公布了数字签名标准，从而使公钥加密技术得到了广泛应用。目前，广泛应用的数字签名算法主要有三种，即RSA签名、DSS(数字签名标准)签名和Hash签名。这三种算法可单独使用，也可综合在一起使用。数字签名是通过密码算法对数据进行加密/解密变换实现的，用DES算法、RSA算法都可实现数字签名。

用RSA或其他公开密钥密码算法的最大方便是没有密钥分配问题(网络越复杂、网络用户越多，其优点越明显)。因为公开密钥加密使用两个不同的密钥，其中有一个是公开的，另一个是保密的(私钥)。公开密钥可以保存在系统目录内、未加密的电子邮件中、电话号码簿或公告牌里，网上的任何用户都可获得公开密钥。而私有密钥是用户专用的，由用户本身持有，它可以对由公开密钥加密的信息进行解密。

一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。数字签名是非对称密钥加密技术与数字摘要技术的应用，其机制需要实现以下几个目的：

(1) 消息源认证：消息的接受者通过签名可以确信消息确实来自声明的发送者。

(2) 不可伪造：签名应是独一无二的，其他人无法假冒和伪造。

(3) 不可重用：签名是消息的一部分，不能被挪用到其他的文件上。

(4) 不可抵赖：签名者事后不能否认自己签过的文件。

DSS数字签名是由美国国家标准化研究院和国家安全局共同开发的。由于DSS是由美国政府颁布实施的，只是一个签名系统，而且美国政府不提倡使用任何削弱政府窃听能力的加密软件，认为这才符合美国的国家利益，因此，DSS主要用于与美国政府做生意的公司，其他公司则较少使用。

2. 单向散列函数

单向散列函数，又称为单向Hash函数、杂凑函数，就是把任意长的输入消息串变化成固定长的输出串且由输出串难以得到输入串的一种函数。这个输出串称为该消息的散列值。一般用于产生消息摘要，密钥加密等。

1) 一个安全的单向散列函数应该满足的几个条件

(1) 输入长度是任意的；

(2) 输出长度是固定的，根据目前的计算技术应至少取128bits长，以便抵抗攻击；

(3) 对每一个给定的输入，计算输出即散列值是很容易的；

(4) 给定散列函数的描述，找到两个不同的输入消息杂凑到同一个值是计算上不可行的，或给定杂凑函数的描述和一个随机选择的消息，找到另一个与该消息不同的消息使得它们杂凑到同一个值是计算上不可行的。

2) 常见单向散列函数(Hash函数)

(1) MD5(Message Digest Algorithm 5)：是RSA数据安全公司开发的一种单向散列算法，MD5被广泛使用，可以用来把不同长度的数据块进行暗码运算成一个128位的数据。

(2) SHA(Secure Hash Algorithm)这是一种较新的散列算法，可以对任意长度的数据

运算生成一个 160 位的数据。

(3) MAC(Message Authentication Code)：消息认证代码，是一种使用密钥的单向函数，可以用它们在系统上或用户之间认证文件或消息。HMAC(用于消息认证的密钥散列法)就是这种函数的一个例子。

(4) CRC(Cyclic Redundancy Check)：循环冗余校验码，CRC 校验由于实现简单，检错能力强，被广泛使用在各种数据校验应用中。占用系统资源少，用软硬件均能实现，是进行数据传输差错检测的一种很好的手段(CRC 并不是严格意义上的散列算法，但它的作用与散列算法大致相同，所以也归入此类)。

3. 数字签名过程

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接受者。接受者只有用发送者的公钥才能解密被加密的摘要信息，然后用 HASH 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

发送报文时，发送方用一个哈希函数从报文文本中生成报文摘要，然后用自己的私人密钥对这个摘要进行加密，这个加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接受方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要，然后再用发送方的公用密钥来对报文附加的数字签名进行解密，如果这两个摘要相同，那么接收方就能确认该数字签名是发送方的，如图 3-9 所示。

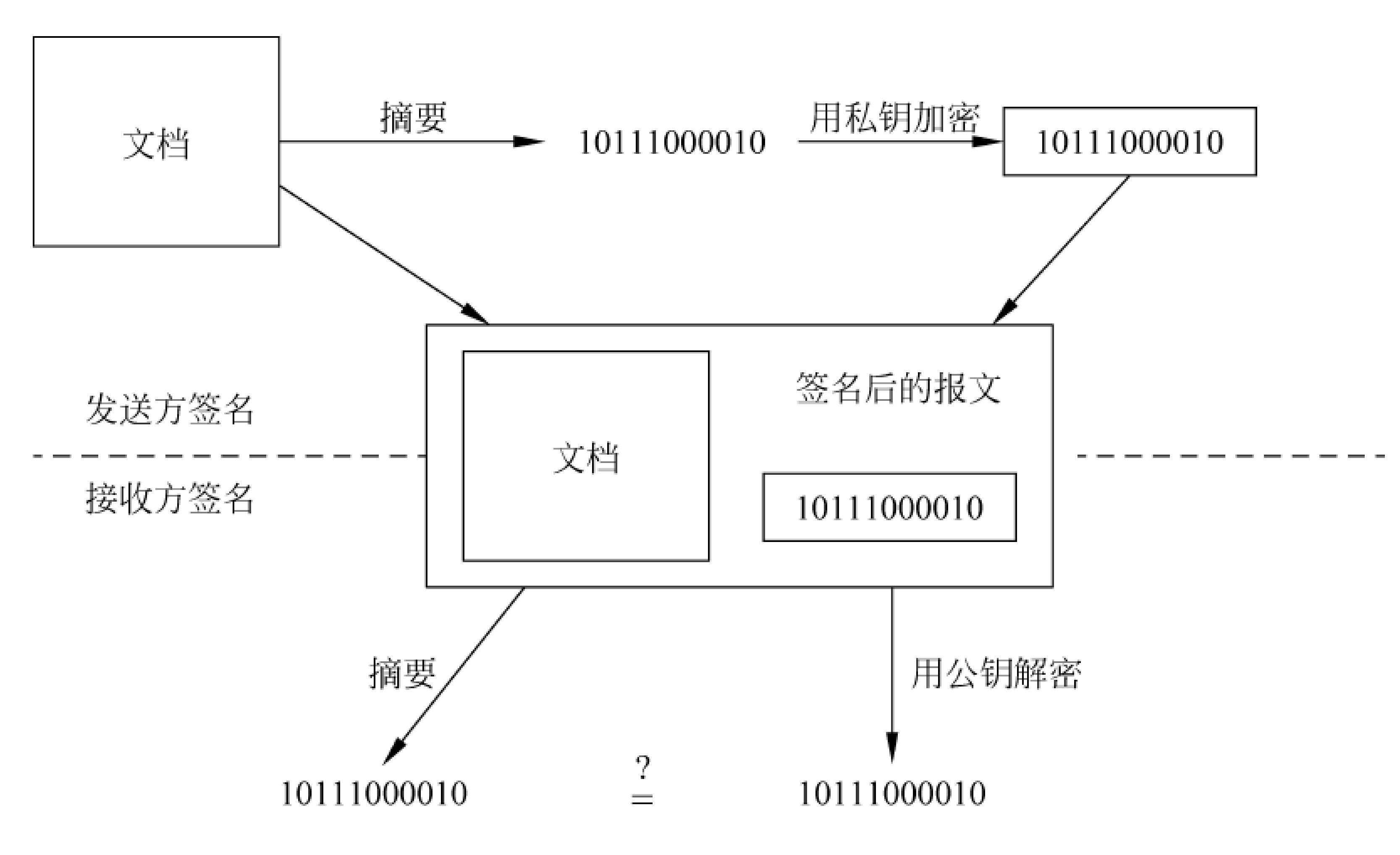


图 3-9　数字签名

数字签名有两方面的作用：一是能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名；二是数字签名能确定消息的完整性。因为数字签名的特点是它代表了文件的特征，文件如果发生改变，数字签名的值也将发生变化。不同的文件将得到不同的数字签名。一次数字签名涉及一个哈希函数、发送者的公钥、发送者的私钥。

4. 数字签名的原理特点

每个人都有两条“钥匙”(数字身份),其中一条钥匙只有她/他本人知道(密钥),另一条钥匙是公开的(公钥)。签名的时候用密钥,验证签名的时候用公钥。又因为任何人都可以落款声称她/他就是你,所以公钥必须由接受者信任的人(身份认证机构)来注册。注册后身份认证机构给用户发一个数字证书。对文件签名后,把此数字证书连同文件及签名一起发给接受者,接受者向身份认证机构求证是否真的是用你的密钥签发的文件。

在通信中使用数字签名一般基于以下原因:

1) 鉴权

公钥加密系统允许任何人在发送信息时使用公钥进行加密,数字签名能够让信息接收者确认发送者的身份。当然,接收者不可能百分之百确信发送者的真实身份,而只能在密码系统未被破译的情况下才能有理由确信。

鉴权的重要性在财务数据上表现得尤为突出。举个例子,假设一家银行将指令由它的分行传输到它的中央管理系统,指令格式是(a,b),其中 a 是账户的账号,而 b 是账户的现有金额。这时一位远程客户可以先存入 100 元,观察传输的结果,然后接二连三地发送格式为(a,b)的指令。这种方法被称作重放攻击。

2) 完整性

传输数据的双方都希望确认消息未在传输的过程中被修改。加密使得第三方想要读取数据十分困难,然而第三方仍然能采取可行的方法在传输的过程中修改数据。一个通俗的例子就是同形攻击:回想一下,还是上面的那家银行从它的分行向它的中央管理系统发送格式为(a,b)的指令,一个远程客户可以现存 100 元,然后拦截传输结果,再传输(a,b3),这样他就立刻变成百万富翁了。

3) 不可抵赖

在密文背景下,抵赖这个词指的是不承认与消息有关的举动(即声称消息来自第三方)。消息的接受方可以通过数字签名来防止所有后续的抵赖行为,因为接收方可以出示签名给别人看来证明信息的来源。

5. 数字签名与信息加密的区别

数字签名使用的是发送方的密钥对,是发送方用自己的私钥对摘要进行加密,接收方用发送方的公钥对数字签名解密,是一对多的关系,表明发送方公司的任何一个贸易伙伴都可以验证数字签名的真伪性;

密钥加密解密过程使用的是接收方的密钥对,是发送方用接收方的公钥加密,接收方用自己的私钥解密,是多对一的关系,表明任何拥有该公司公钥的人都可以向该公司发送密文,但只有该公司才能解密,其他人不能解密。

3.3.3 物联网认证与访问控制

认证指使用者采用某种方式来证明自己确实是自己宣称的某人,网络中的认证主要包括身份认证和消息认证。身份认证可以使通信双方确信对方的身份后交换会话密钥,消息认证主要是接收方希望能够保证其接收的消息确实来自真正的发送方。

在物联网的认证过程中，传感器网络的认证机制是重要的研究部分，无线传感器网络中的认证技术主要包括基于轻量级公钥的认证技术、预共享密钥的认证技术、随机密钥预分布的认证技术、利用辅助信息的认证和基于单向散列函数的认证等。

访问控制是对用户合法使用资源的认证和控制，目前信息系统的访问控制主要是基于角色的访问控制机制（Role-Based Access Control，RBAC）及其扩展模型。RBAC 机制主要由 Sandhu 于 1996 年提出的基本模型 BRAC96 构成，一个用户先由系统分配一个角色，如管理员或普通用户等，登录系统后，根据用户的角色所设置的访问策略实现对资源的访问。显然，同样的角色可以访问控制方法，是基于用户的访问控制。

对物联网而言，末端是感知网络，可能是一个感知结点或一个物体，采用用户角色的形式进行资源的控制显得不够灵活，主要表现在以下 3 点：

(1) 基于角色的访问控制在分布式的网络环境中已呈现出不相适应的地方，如对具有时间约束资源的访问控制，访问控制的多层次适应性等方面需要进一步探讨。

(2) 结点不是用户，而是各类传感器或其他设备，且种类繁多，基于角色的访问控制机制中角色类型无法一一对应这些结点，因此，使 RBAC 机制难以实现。

(3) 物联网主要是信息的感知互动过程，包含了信息的处理、决策和控制等过程，特别是反向控制是物物相连的特征之一，资源的访问呈现动态性和多层次性，而 RBAC 机制中一旦用户被指定为某种角色，他的可访问资源就相对固定了，所以，寻求新的访问控制机制是物联网，也是互联网值得研究的问题。

基于属性的访问控制（Attribute-Based Access Control，ABAC）是近几年研究的热点，如果将角色映射成用户的属性，可以构成 ABAC 与 RBAC 的对等关系，而属性的增加相对简单，同时基于属性的加密算法可以使 ABAC 得以实现。ABAC 方法的问题是对较少的属性来说，加密解密的效率较高，但随着属性数量的增加，加密的密文长度增加，使算法的实用性受到限制，目前有两个发展方向：基于密钥策略和基于密文策略，其目标就是改善基于属性的加密算法的性能。

3.3.4 公钥基础设施——PKI

1. PKI 概述

公钥基础设施（Public Key Infrastructure，PKI）是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。

PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封和双重数字签名等。PKI 是指用公钥概念和技术来实施和提供安全服务的具有普适性的安全基础设施，指任何以公钥技术为基础的安全基础设施都是 PKI，若没有好的非对称算法和好的密钥管理就不可能提供完善的安全服务，不能称为 PKI，即该定义中已经隐含了必须具有的密钥管理功能。

X. 509 标准中，为了区别于权限管理基础设施（Privilege Management Infrastructure，PMI），将 PKI 定义为支持公开密钥管理并能支持认证、加密、完整性和可追究性服务的基

础设施。这个概念与第一个概念相比，不仅仅叙述 PKI 能提供的安全服务，更强调 PKI 必须支持公开密钥的管理。也就是说，仅仅使用公钥技术还能叫做 PKI，还应该提供公开密钥的管理。因为 PMI 仅仅使用公钥技术但并不管理公开密钥，所以 PMI 就可以单独进行描述，而不至于跟公钥证书等概念混淆。

美国国家审计总署在 2001 年和 2003 年的报告中都把 PKI 定义为由硬件、软件、策略和人构成的系统，当完善实施后，能够为敏感通信和交易提供一套信息安全保障，包括保密性、完整性、真实性和不可否认。

2. 基本组成

完整的 PKI 系统必须具有权威认证机构（CA）、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口（API）等基本构成部分，构建 PKI 也将围绕着这 5 大系统来构建。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封和双重数字签名等。

（1）认证机构（CA）。即数字证书的申请签发机关，CA 必须具备权威性的特征。

（2）数字证书库。用于存储已签发的数字证书及公钥，用户可由此获得所需的其他用户的证书及公钥。

（3）密钥备份及恢复系统。如果用户丢失了用于解密数据的密钥，则数据将无法解密，这将造成合法数据丢失。为避免这种情况，PKI 提供备份与恢复密钥的机制。但需注意，密钥的备份与恢复必须由可信的机构来完成，并且，密钥备份与恢复只能针对解密密钥，签名私钥为确保其唯一性而不能够作备份。

（4）证书作废系统。证书作废处理系统是 PKI 的一个必备的组件。与日常生活中的各种身份证件一样，当密钥介质丢失或用户身份变更等时，证书有效期内也可能作废，即 PKI 必须提供作废证书的一系列机制。

（5）应用接口（API）。PKI 的价值在于使用户能够方便地使用加密、数字签名等安全服务，因此一个完整的 PKI 必须提供良好的应用接口系统，使得各种各样的应用能够以安全一致、可信的方式与 PKI 交互，确保安全网络环境的完整性和易用性。

通常来说，CA 是证书的签发机构，它是 PKI 的核心。众所周知，构建密码服务系统的核心内容是如何实现密钥管理。公钥体制涉及一对密钥（即私钥和公钥），私钥只由用户独立掌握，无须在网上传输，而公钥则是公开的，需要在网上传送，故公钥体制的密钥管理主要是针对公钥的管理问题，目前较好的解决方案是数字证书机制。

3. 目标

PKI 是一种基础设施，其目标就是要充分利用公钥密码学的理论基础，建立起一种普遍适用的基础设施，为各种网络应用提供全面的安全服务。公开密钥密码为我们提供了一种非对称性质，使得安全的数字签名和开放的签名验证成为可能。而这种优秀技术的使用却面临着理解困难、实施难度大等问题。正如让电视机的开发者理解和维护发电厂有一定的难度一样，要让每一个应用程序的开发者完全正确地理解和实施基于公开密钥密码的安全有一定的难度。PKI 希望通过一种专业的基础设施的开发，让网络应用系统的开发人员从烦琐的密码技术中解脱出来，而同时享有完善的安全服务。

将 PKI 在网络信息空间的地位与电力基础设施在工业生活中的地位进行类比可以更好地理解 PKI。电力基础设施通过伸到用户的标准插座为用户提供能源，而 PKI 通过延伸用户本地的接口为各种应用提供安全的服务。有了 PKI，安全应用程序的开发者可以不用再关心那些复杂的数学运算和模型，而直接按照标准使用一种插座(接口)。正如电冰箱的开发者不用关心发电机的原理和构造一样，只要开发出符合电力基础设施接口标准的应用设备，就可以享受基础设施提供的能源。

PKI 与应用的分离也是 PKI 作为基础设施的重要标志。正如电力基础设施与电器的分离一样，网络应用与安全基础实现了分离，有利于网络应用更快地发展，也有利于安全基础设施更好地建设。正是由于 PKI 与其他应用能够很好地分离，才使得我们能够将之称为基础设施，PKI 也才能从千差万别的安全应用中独立出来，才能有效地、独立地发展壮大。PKI 与网络应用的分离实际上就是网络社会的一次"社会分工"，这种分工可能会成为网络应用发展史上的重要里程碑。

4. 内容

PKI 在公开密钥密码的基础上，主要解决密钥属于谁，即密钥认证的问题。通过数字证书，PKI 很好地证明了公钥是谁的，PKI 的核心技术就围绕着数字证书的申请、颁发、使用与撤销等整个生命周期展开，其中，证书撤销是 PKI 中最容易被忽视，但却是很关键的技术之一，也是基础设施必须提供的一项服务。

PKI 技术的研究对象包括数字证书、数字证书认证中心、证书持有者和证书用户，以及为了更好地成为基础设施而必须具备的证书注册机构、证书存储和查询服务器、证书状态查询服务器、证书验证服务器等。

PKI 作为基础设施，两个或多个 PKI 管理域的互连就非常重要。PKI 域间如何互联，如何更好地互联就是建设一个无缝的大范围的网络应用的关键。在 PKI 互连过程中，PKI 关键设备之间，PKI 末端用户之间，网络应用与 PKI 系统之间的互操作与接口技术就是 PKI 发展的重要保证，也是 PKI 技术的研究重点。

5. 优势

PKI 作为一种安全技术，已经深入到网络的各个层面。这从一个侧面反映了 PKI 强大的生命力和无与伦比的技术优势。PKI 的灵魂来源于公钥密码技术，这种技术使得"知其然不知其所以然"成为一种可以证明的状态，使得网络上的数字签名有了理论上的安全保障。围绕着如何用好这种非对称密码技术，数字证书破壳而出，并成为 PKI 中最为核心的元素。

PKI 的优势主要表现在：

(1) 采用公开密钥密码技术，能够支持可公开验证并无法仿冒的数字签名，从而在支持可追究的服务上具有不可替代的优势。这种可追究的服务也为原发数据完整性提供了更高级别的担保。支持可以公开地进行验证，或者说任意的第三方可验证，能更好地保护弱势个体，完善平等的网络系统间的信息和操作的可追究性。

(2) 由于密码技术的采用，保护机密性是 PKI 最得天独厚的优点。PKI 不仅能够为相互认识的实体之间提供机密性服务，同时也可以为陌生的用户之间的通信提供保密支持。

(3) 由于数字证书可以由用户独立验证，不需要在线查询，原理上能够保证服务范围的

无限制扩张，这使得 PKI 能够成为一种服务巨大用户群的基础设施。PKI 采用数字证书方式进行服务，即通过第三方颁发的数字证书证明末端实体的密钥，而不是在线查询或在线分发。这种密钥管理方式突破了过去安全验证服务必须在线的限制。

（4）PKI 提供了证书的撤销机制，从而使得其应用领域不受具体应用的限制，撤销机制提供了在意外情况下的补救措施，在各种安全环境下都可以让用户更加放心。另外，因为有撤销技术，不论是永远不变的身份，还是经常变换的角色，都可以得到 PKI 的服务而不用担心被窃后身份或角色被永远作废或被他人恶意盗用。为用户提供“改正错误”或“后悔”的途径是良好工程设计中必须的一环。

（5）PKI 具有极强的互联能力。不论是上下级的领导关系，还是平等的第三方信任关系，PKI 都能够按照人类世界的信任方式进行多种形式的互联互通，从而使 PKI 能够很好地服务于符合人类习惯的大型网络信息系统。PKI 中各种互联技术的结合使建设一个复杂的网络信任体系成为可能。PKI 的互联技术为消除网络世界的信任孤岛提供了充足的技术保障。

3.4　常用安全协议

3.4.1　Kerberos 协议

Kerberos 协议是一种网络认证的协议，其工作的原理是通过密钥，对客户端或者服务器提供一个认证服务，与传统的认证协议相比，Kerberos 协议不需要物理安全，只要通过认证，就可以随意的读取和修改数据库。因此，这种协议被广泛地应用在第三方认证服务领域，该协议在 TCP/IP 协议栈中，处于 UDP 和 TCP 的上层，与 HTTP 处于同一个级别。在具体认证的过程中，采用数据加密算法进行认证，用户机首先要发出相应的请求，然后安装服务器的证书文件，服务器如果能够读取正确的用户密钥，那么就可以通过相应的认证，这个证书文件还可以为经过认证后的通信进行加密，保证通信内容的安全。目前，很多服务器都采用这个协议进行加密，以此来保证网络的安全，尤其是一些含有重要内容的通信，以及需要相应的身份才能访问数据的系统，Kerberos 协议可以很好地防止连接和窃听，虽然该协议的安全性较高，可以为不同的服务提供单独的认证，但这种认证体系不会验证物理地址，因此无法检验用户的真实性，如果密钥的数量过多，那么对认证服务器的性能，会有很高的要求。

3.4.2　SET 协议

SET 是 Secure Electronic Transaction 的缩写，中文名为安全电子交易协议，该协议是随着电子支付的普及应用，逐渐产生的一种安全协议，由于其可以很好地处理用户、商户和银行之间的关系，在 B2C 等网站上得到了广泛的应用，经过了多年的使用，已经成为了信用卡网上交易的国际标准。在 TCP/IP 协议栈中，SET 协议处于 HTTP 的上层，在实际的网上交易中，由于用户与商家都是经过网络沟通，具有一定的虚拟性，在用户确定订单之后，商家希望用户可以填写更多真实的信息，而用户则希望一些私密的账户信息等可以保密，但是

由于双方不够了解，经常会出现矛盾甚至是欺诈的现象，而 SET 协议的应用可以很好地解决这个问题，利用这种协议对双方进行认证，用户信用卡等信息就不会被商家知道。SET 协议的安全系数很高，所有参与的用户都必须先安装证书，以此来识别自己的身份，可以很好地防止欺诈现象的发生，但是由于这种算法自身非常复杂，要想使用这种算法需要较高的成本，而且对此加密对服务性能的要求很高，在使用的过程中，必须安装相应的插件和软件。

3.4.3 SSL 协议

SSL 协议是网景公司在开发浏览器的过程中，研发的一种安全协议，因此该协议主要是为了保证网络数据传输的安全，采用数据加密技术，可以很好地防止数据在上行或下行的过程中被窃取。因此，现在的 Web 浏览器，基本上都支持该协议，SSL 协议在 TCP/IP 协议栈中处于 TCP 和 HTTP 之间，SSL 协议可以选择多种加密算法来进行认证。SSL 协议的认证是双向的，首先就是服务器的认证，客户机要向服务发出请求信息，服务器接收到用户的请求后，会返回用于生成密钥的相关信息，用户收到这个信息后就可以生成密钥，完成对服务器的认证，最后服务器还要向客户机发送一个提问，客户机返回相应的数据后，才算完成双方的认证。SSL 协议的应用非常广泛，几乎所有涉及 Web 通信的领域，都可以采用该协议来保证网络的安全，尤其是该协议的设置非常简单，只需要少量的成本，不需要安装任何的插件和软件，但是该协议只能保证传输过程的安全。

3.4.4 SHTTP 协议

SHTTP 是 Secure HyperText Transfer Protocal 的缩写，中文名为安全超文本转换协议，该协议是在传统 HTTP 的基础上，为了保证网络的安全性，研发的一种新的网络安全协议，SHTTP 协议的应用，可以很好地兼容 HTTP 的程序，这种协议可以提供多种安全措施，能够满足互联网上不同用户的需求，SHTTP 与 HTTP 处于同一协议层中。SHTTP 可以通过不同的算法来保证数据的安全，如常见的 RSA、DES 等，在实际的应用中，可以与 SSL 协议共同来保证数据传输的安全，也可以协同 SET 协议等，进行具体功能上的保护，虽然这种协议具有很高的安全性，但是实现起来具有较大的难度，因此目前还没有得到普及应用。

3.5 本章小结

本章介绍了密码学的历史、密码系统的概念、密码的分类，重点介绍了几种常用加密技术原理及其应用，最后介绍了几种安全协议。

密码系统又称为密码体制，是指能完整地解决信息安全中的机密性、数据完整性、认证、身份识别及不可抵赖等问题中的一个或几个的一个系统。其目的是人们能够使用不安全信道进行安全的通信。

加密技术主要分为对称加密算法和非对称加密算法。对称加密算法指加密和解密使用相同密钥的加密算法，就是加密密钥能够从解密密钥中推算出来，同时解密密钥也可以从

加密密钥中推算出来。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA 和 AES。非对称加密算法是指加密密钥与解密密钥是不同的，一个称为公开密钥，另一个称为私人密钥(或秘密密钥)，因此这种密码体系也称为公钥密码体系。公钥密码体制的算法中最著名的代表是 RSA 系统，此外还有椭圆曲线、背包密码和 ElGamal 算法等。

基于数据加密的应用技术包括鉴别、数字签名、物联网认证与访问控制以及公钥基础设施等。

常用安全协议有 Kerberos 协议、SET 协议、SSL 协议和 SHTTP 协议等。

复习思考题

1. 简述密码学的定义和作用。
2. 古典密码学主要分成哪几种类型？请详述其中一种。
3. 什么是非对称加密，有哪些特点？请介绍几种非对称加密算法。
4. 什么是公钥加密，有哪些特点？请介绍几种公钥加密算法。
5. 什么是单向散列函数？请举例说出有哪些属于单向散列函数。
6. 简述数字签名技术的原理。
7. 数字签名与加密技术在密钥对的使用上有什么区别？
8. PKI 的优势主要表现在哪些方面？
9. 网络中的认证包括哪些方面？什么是物联网认证？
10. 目前信息系统的访问控制有哪几种？分别简述其特点。
11. 常用的网络协议有哪些？请阐述每一种协议的工作原理。

第4章 感知层安全技术

4.1 RFID安全技术

4.1.1 RFID系统的组成部分

射频识别(Radio Frequency Identification,RFID)技术是一种非接触式自动识别技术。它通过无线射频方式自动识别特定目标的电子标签,并读写标签中的相关信息。

RFID技术可以识别高速运动的目标对象,例如行驶中的汽车,并可以同时识别多个标签,能够快速地进行物品的追踪和管理,具有可靠性高、保密性强、成本低廉等特点。它广泛应用于仓库管理、物品追踪、防伪、物流配送、过程控制、访问控制、门禁、自动收费、供应链管理、图书管理等领域。

RFID系统的组成部分如图4-1所示。

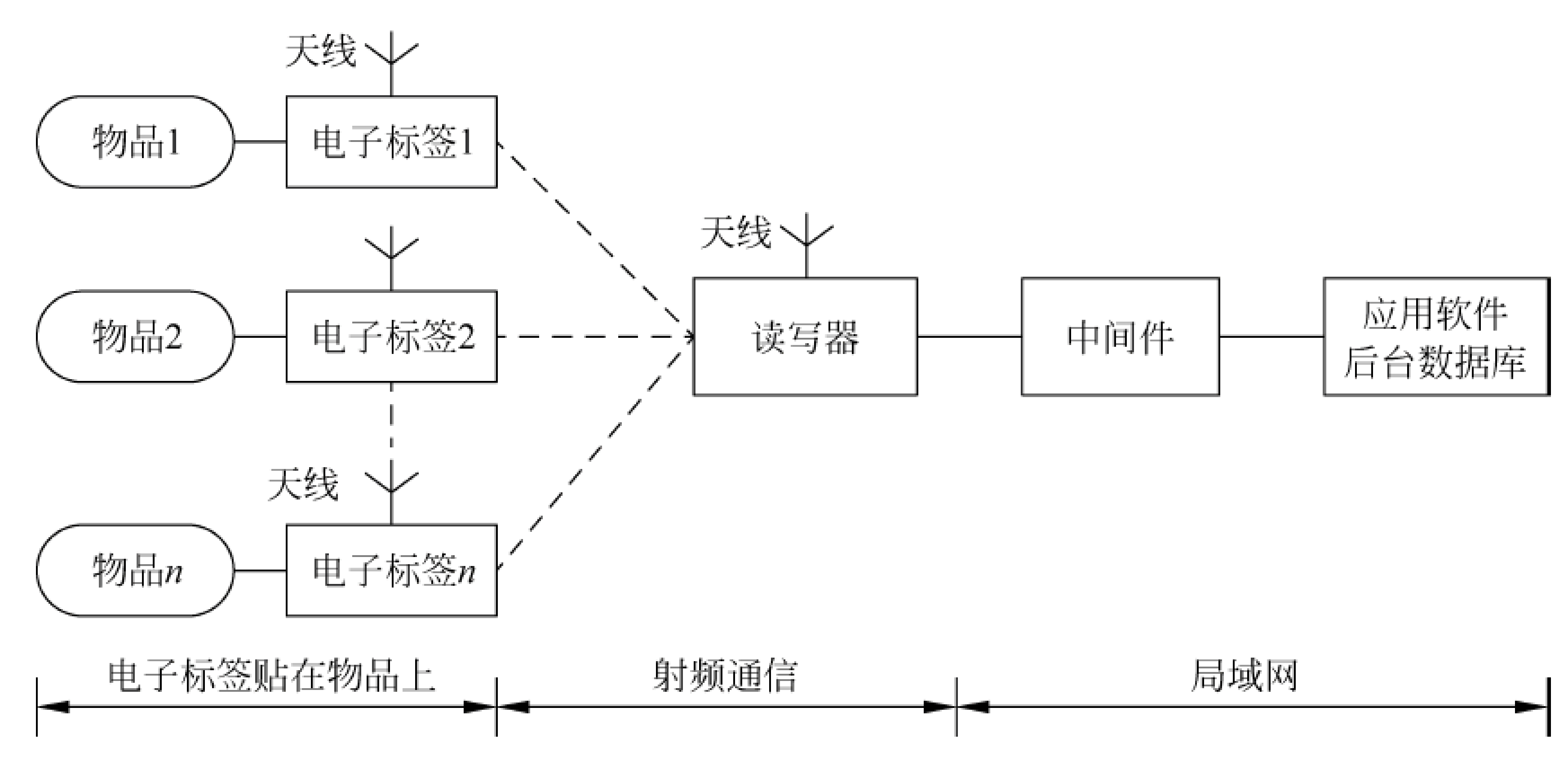


图4-1 RFID系统的基本组成部分

一套完整的RFID系统,通常由物品(Physical thing)、电子标签(Tag)、天线(Antenna)、读写器(Reader and Writer)、中间件(Middleware)和应用软件(Application Software)等六个部分组成。各个组成部分的主要功能如下:

1. 物品(Physical thing)

物品是指物理世界中实实在在的物体,如服装、食物、汽车、文具、书刊、家具等各种各样的物品。在物联网中,这些物品都是可以互联的。

2. 电子标签(Tag)

RFID 标签俗称电子标签(Tag),也称为应答器(Responder),根据工作方式,电子标签可以分为主动式(有源)和被动式(无源)两大类。在本书中,仅仅介绍常用的被动式电子标签。

被动式 RFID 标签由标签芯片和标签天线(或线圈)组成,利用电感耦合或电磁反向散射耦合原理实现与读写器之间的通信。RFID 标签中存储一个唯一编码,通常是一个 64 位二进制数、96 位二进制数甚至位数更多的二进制数,其地址空间大大高于条形码所能提供的空间,因此可以实现全球唯一的物品编码。当 RFID 标签进入读写器的作用区域,就可以根据电感耦合原理(近场作用范围内)或电磁反向散射耦合原理(远场作用范围内)在标签天线两端产生感应电势差,并在标签芯片通路中形成微弱电流,如果这个电流强度超过一个阈值,就将激活 RFID 标签芯片电路工作,从而对标签芯片中的存储器进行读/写操作,微控制器还可以进一步加入诸如密码或防碰撞算法等复杂功能。RFID 标签芯片的内部结构主要包括射频前端、模拟前端、数字基带处理单元和 E^2PROM 存储单元四个部分。

3. 天线(Antenna)

天线是 RFID 标签和读写器之间实现射频信号空间传播和建立无线通信连接的设备。RFID 系统中包括两类天线,一类是 RFID 标签上的天线,由于它已经和 RFID 标签集成为一体,因此不再单独讨论;另一类是读写器天线,既可以内置于读写器中,也可以通过同轴电缆与读写器的射频输出端口相连。目前的天线产品大多采用收发分离技术来实现发射和接收功能的集成。天线在 RFID 系统中的重要性往往被人们所忽视,在实际应用中,天线性能的优劣是影响 RFID 系统识别质量的主要因素。高性能的天线不仅要求具有良好的阻抗匹配特性,还需要根据应用环境的特点对方向特性、极化特性和频率特性等进行专门设计。

4. 读写器(Reader and Writer)

读写器也称为阅读器或询问器(Interrogator),它是对 RFID 标签进行读/写操作的设备,主要包括射频模块和数字信号处理单元两部分。读写器是 RFID 系统中最重要的工作单元。

一方面,RFID 标签返回的微弱电磁信号通过天线进入读写器的射频模块中转换为数字信号,再经过读写器的数字信号处理单元对其进行必要的加工整形,最后从中解调出返回的信息,完成对 RFID 标签的识别或读/写操作;另一方面,上层中间件及应用软件与读写器进行交互,实现操作指令的执行和数据汇总上传。

当上传数据时,读写器会对 RFID 标签原始数据进行去重过滤或简单的条件过滤,将其加工为读写器数据后再上传,以减少与中间件及应用软件之间数据交换的流量,因此在很多读写器中还集成了微处理器和嵌入式系统,实现一部分中间件的功能,如信号状态控制、奇

偶位错误校验与修正等。未来的读写器呈现出智能化、小型化和集成化趋势，还将具备更加强大的前端控制功能，例如直接与工业现场的其他设备进行交互甚至是作为控制器进行在线调度。在物联网中，读写器将成为同时具有通信、控制和计算（Communication、Control、Computing）功能的C3核心设备。

5. 中间件（Middleware）

中间件是一种面向消息的、可以接受应用软件端发出的请求、对指定的一个或者多个读写器发起操作并接收、处理后向应用软件返回结果数据的特殊软件。中间件在RFID应用中除了可以屏蔽底层硬件带来的多种业务场景、硬件接口、适用标准等造成的可靠性和稳定性问题，还可以为上层的应用软件提供多层、分布式、异构的信息环境下业务信息和管理信息的协同。中间件还可以根据一个或多个读写器的读写器事件进行过滤、聚合和计算，抽象出对应用软件有意义的业务逻辑信息构成业务事件，以满足来自多个客户端的检索、发布/订阅和控制请求。

6. 应用软件（Application Software）

应用软件采用位于后台的数据库管理系统来实现其管理功能，它提供直接面向RFID应用最终用户的人机交互界面，协助使用者完成对读写器的指令操作，以及对中间件的逻辑设置，逐级将RFID标签上的原始数据转化为便于使用者理解的业务数据，并使用可视化界面进行展示。由于应用软件需要针对不同应用领域的用户专门编制，因此很难具有通用性。从应用评价标准来说，使用者在应用软件界面上的用户体验，是判断一个RFID应用系统成功与否的决定性因素。

4.1.2 RFID系统的工作原理

如前所述，一套完整的RFID系统，由物品、电子标签、天线、读写器、中间件和应用软件等部分组成。

在基于RFID技术的物联网系统中，标签与读写器之间是通过射频信号进行通信的，而读写器与应用系统之间是通过局域网进行通信的。

RFID系统的工作原理是读写器发射某个特定频率的无线电波，把能量传送给电子标签，用以驱动电子标签电路工作，将其内部的数据送出，此时读写器便按次序接收并解读数据，然后送给应用系统作相应的处理。

当电子标签进入磁场后，读写器发出射频信号，电子标签凭借天线感应电流所获得的能量，发送出存储在芯片中的产品信息（Passive Tag，被动标签），或者由电子标签主动发送某一频率的信号（Active Tag，有源标签或主动标签），读写器读取信息并解码后，送至中间件进行有关数据处理。

以RFID读写器与电子标签之间的通信及能量感应方式来分类，RFID大致上可以分成两类：感应耦合（Inductive Coupling）和后向散射耦合（Backscatter Coupling）。通常，低频的RFID系统大都采用感应耦合方式，而较高频的RFID系统大多采用后向散射耦合方式。

读写器是RFID系统信息控制和处理中心。按照所采用的结构和技术的不同，读写器可以是读出装置，也可以是读/写装置。读写器通常由耦合模块、收发模块、控制模块和接口

单元组成。读写器与电子标签之间一般采用半双工通信方式进行信息交换,同时读写器通过耦合给无源电子标签提供能量和信号。

在实际应用中,可进一步通过有线局域网(Wired Local Area Network)或无线局域网(Wireless Local Area Network)等实现对标签提供的物体标识信息的采集、处理和远程传送等管理功能。电子标签是RFID系统的信息载体,目前电子标签大多是由耦合元件(线圈、微带天线等)和微芯片组成无源单元。

RFID射频识别系统的基本工作方式可以分为全双工(Full Duplex)、半双工(Half Duplex)系统和时序(SEQ)系统。

全双工表示电子标签与读写器之间可在同一时刻互相传送信息;半双工表示电子标签与读写器之间也可以双向传送信息,但收发双方必须轮流工作,在同一时刻只能向一个方向传送信息。

在全双工和半双工系统中,电子标签的响应是读写器通过电磁波发送出去的。因为与读写器发出的电磁波信号相比,在电子标签接收天线上的电磁波信号很微弱,所以必须使用合适的传输方法,以便把电子标签的信号与读写器的信号区别开来。传输方法有负载反射调制技术和时序方法两种。

在实际应用中,对从电子标签到读写器之间的数据传输,一般采用负载反射调制技术,将电子标签数据加载到反射回波上。

时序方法则与负载反射调制技术相反,读写器发射出的电磁波短时间周期性地断开。这些时间间隔被电子标签识别出来,并被用于从电子标签到读写器的数据传输。实际上,这是一种典型的雷达工作方式。时序方法的缺点是:在读写器发送间歇时,电子标签的能量供应中断,这就必须通过配备足够大的辅助电池的方法来提供电源。

读写器发送信号时使用的频率称为RFID系统的工作频率。按工作频率来划分,RFID系统可以分为低频系统和高频系统。

低频RFID系统一般指其工作频率小于30MHz,典型的工作频率为:125KHz、225KHz、13.56MHz等,工作在这些频率的射频识别系统一般都适用于相应的国际标准。低频RFID系统的基本特点是电子标签的成本较低、电子标签内保存的数据量较少、阅读距离较短、电子标签外形多样(卡状、环组、纽扣状、笔状)、阅读天线方向性不强等。

高频RFID系统一般指其工作频率大于400MHz,典型的工作频率为:915MHz、2.45GHz、5.8GHz等。高频RFID系统在这些频率上也得到了众多国际标准的支持。高频RFID系统的基本特点是电子标签及读写器的成本比较高、电子标签内保存的数据量较大、阅读距离较远(可达几米至十几米)、适应于高速运动的物体、外形一般为卡状、阅读天线和电子标签天线都有较强的方向性等。

4.1.3 RFID系统的安全威胁

随着RFID技术的快速发展,它在物联网中的应用已经远远超出了原有计算机系统的范围。其安全问题也成为一个业界广泛关注的问题,其主要原因包括以下几个方面。

1. 标签计算能力比较弱

RFID标签在计算能力和功耗方面具有特有的局限性,RFID标签的存储空间非常少,

最廉价的标签,只有 64～128 位的存储空间,仅仅可以存放唯一的标识符。由于标签本身的成本所限,标签本身较难具备足够的安全能力,很容易被攻击者操控,攻击者可以利用合法的读写器或者自行构造的一个读写器,直接与 RFID 标签进行通信,读取、篡改甚至删除标签内所存储的数据。在没有足够可信任的安全机制的保护下,标签的安全性、有效性、完整性、可用性和真实性都难以得到保障。

2. 无线网络的脆弱性

标签层和读写器层采用无线射频信号进行通信,在通信的过程中没有任何物理或者可见的接触,而无线网络固有的脆弱性使系统很容易受到各种形式的攻击。在给应用系统数据采集提供灵活性和方便性的同时,RFID 系统传递的信息也会暴露在环境中。

3. 业务应用的隐私安全

在传统的网络中,网络层的安全和业务层的安全是相互独立的,而在物联网中,网络连接和业务使用是紧密结合的。物联网中传输信息的安全性和隐私性问题,也成为了制约物联网进一步发展的重要因素。

根据 RFID 物联网的系统结构,可以把物联网面临的威胁和攻击分为两类:第一类是针对物联网系统的实体的威胁,主要是针对标签、读写器和应用系统的攻击;另一类是针对物联网中的通信过程的威胁,包括针对射频通信和互联网通信的攻击。

4.1.4 RFID 系统的总体安全需求

一个比较完整的 RFID 系统安全解决方案,应当综合考虑物联网系统中的实体安全和通信安全,并满足机密性、完整性、可用性、可审计性和隐私性等安全需求。

1. 机密性

机密性是指电子标签内部的数据和电子标签与读写器之间通信的数据不能被非法获取,即使被非法获取也不能被理解。机密性保证信息只能被授权访问,一个 RFID 电子标签不应当向未授权的读写器泄露任何敏感的信息。机密性对于公交卡、电子钱包等包含敏感数据的电子标签非常重要。

2. 完整性

完整性是指电子标签内部数据及其与读写器之间的通信数据不能被非法篡改,即使被篡改也能够被检测到。篡改数据是欺骗行为,大多数 RFID 系统都需要保证数据的完整性。在 RFID 系统中,通常使用消息认证码来进行数据完整性的检验,即使用带有共享密钥的散列算法,将共享密钥和待检验的消息连接在一起进行散列运算,对数据的任何改动都会导致消息认证码的值产生变化,从而发现攻击行为。

3. 可用性

可用性是指系统在需要的时候能够被合法使用,攻击者不能限制合法用户的使用。对于 RFID 系统来说,由于空中接口反射信号微弱以及防冲突协议的脆弱性等原因,可用性受

到破坏的可能性比较大。在公众场合，电子标签的可用性很容易被屏蔽、遮盖、撕毁等手段破坏，因此，在系统设计中应加以重视。考虑到节能的要求，一个合理的 RFID 安全方案中安全协议和算法的设计都不应当过于复杂，并尽可能地避开公钥运算，计算开销、存储容量和通信能力也应当充分考虑 RFID 系统资源有限的特点，即安全性设计方案不应当限制 RFID 系统的可用性，并能够有效防止攻击者对电子标签资源的恶意消耗。

4. 可审计性

对于 RFID 系统而言，可审计性主要是要保证读写器、电子标签及其数据是真实可信的，要保证标签被读取或者被写入的记录可以被追踪。预防伪造和假冒的读写器、假冒的电子标签及其数据。由于电子标签数据要被送到后台系统中作进一步的处理，虚假数据可能导致较大的损失，因此要求电子标签及其数据是真实的。攻击者可能伪造电子标签，也可能通过某种方式隐藏电子标签，使读写器无法发现该标签，从而成功地实施物品转移，读写器必须通过身份认证才能确信消息是从合法的电子标签处发送过来的。

5. 隐私性

隐私性是针对个人携带粘贴了电子标签的物品而产生的需求。RFID 标签可能会泄露使用者的个人喜好、消费习惯、行踪等隐私信息。隐私性可以分为信息隐私、位置隐私和交易隐私等类型。信息隐私是指用户相关的非公开信息不能被获取或者推断出来；位置隐私是指携带电子标签的用户不能被跟踪和定位；交易隐私是指电子标签在与系统交换数据时，或者单个用户新增某个标签时，或者用户失去某个标签时，产生的交易信息不能被获取。

4.1.5　RFID 系统各组成部分的安全需求

1. 电子标签

在电子标签中需要保护数据包括 4 种类型：标签标识；用于认证和控制标签内数据访问的密钥；标签内的业务数据；标签的执行代码。

电子标签的安全需求包括机密性、完整性、可用性和可审计性四个方面。

1）机密性

机密性是指标签内的数据不能被未授权的用户访问。尤其是标签标识，由于其相对固定并与物理世界中的人和物体紧密关联，因此标签标识的机密性作为隐私问题而被特别关注。在考虑保护标签机密性时，除了传统安全领域的安全策略之外，还需要考虑标签的低成本、低性能的特性。由于标签体积很小且成本很低，因此其计算能力有限，在考虑引入传统的加密机制、认证机制和访问控制时，应充分考虑其实现时的计算能力问题。

2）完整性

完整性是指标签中的数据不能被未授权的用户所修改。标签的完整性主要用于保护标签中的业务数据不受恶意修改，因为这些数据通常包括大量与业务相关的信息。特别是当标签用于银行、股市和保险等金融领域时，标签中的数据往往具有经济意义。

3）可用性

可用性是指标签中的数据和功能可以进行正常读取和响应。标签一般都粘贴在物品的

表面或嵌入在物品内部，而粘贴在物品上的标签很容易被毁坏。另外，Kill 命令可以删除标签中的部分或者全部数据，甚至使之完全失效。Kill 命令是为了保护用户的隐私而制订的，攻击者有可能利用这一命令毁坏标签。因此，应保证标签的可用性，使之能够正常响应读写器的请求。

4）可审计性

可审计性是指对标签的任何读写操作都能被审计追踪，从而保证标签的可审计性。

2. 读写器

在读写器中需要保护的数据主要包括 3 种类型：与标签进行相互认证的密钥；与标签相关的数据；读写器的执行代码。

读写器的安全需求也包括机密性、完整性、可用性和可审计性四个方面。

1）机密性

机密性是指读写器中的数据只能被授权用户访问。特别是与标签进行相互认证的密钥，如果密钥信息泄漏，攻击者很可能通过假冒读写器与标签进行通信，因此必须保证读写器中的密钥的机密性。由于读写器不需要严格考虑成本，因此可以沿用传统的加密机制来保护机密性。

2）完整性

完整性是指读写器中的数据仅能被授权用户修改。特别是要保护与标签相关的信息不被攻击者修改，因为这些数据与业务密切相关。

3）可用性

可用性是指读写器能够正常发送请求并且能够响应标签的回复。攻击者可能利用或毁坏读写器，因此需要保证读写器的可用性。

4）可审计性

可审计性是指要保证读写器读取标签或者写入标签的记录都可以被监测、追踪和审计。

3. 应用软件

在应用软件中需要保护的数据包括 4 种类型：与标签相关的数据；与用户相关的数据；与业务应用相关的数据；代码。

应用软件的安全需求同样包括机密性、完整性、可用性和可审计性等四个方面。

1）机密性

机密性是指应用系统中的数据不能被未授权用户访问。特别是与标签相关和与用户相关的信息，这些信息往往涉及用户的隐私，通常都保存在后台数据库中，一旦被攻击者获取，使用者的隐私将无法得到保障。此外，还必须保证与业务应用相关的数据的机密性，因为攻击者很可能通过分析这些数据来追踪用户的行踪，甚至分析用户的消费习惯。

2）完整性

完整性是指应用系统中的数据不能被未授权用户篡改。特别是与用户相关的数据和业务数据，一旦被攻击者篡改，可能造成很大的经济损失。

3）可用性

可用性是指保证应用系统正常运转，满足用户的需求。

4）可审计性

可审计性是指保证应用系统可以被监测、追踪和审计。

4. 射频通信模块

射频通信模块需要保护的对象包括通信数据和通信信道。

射频通信模块的安全需求也包括机密性、完整性、可用性和可审计性等四个方面。

1）机密性

机密性是指保护射频通信数据的机密性。射频通信模块是通过无线射频信号进行通信的，攻击者可以通过窃听分析微处理器正常工作过程中产生的各种电磁特征，来获得标签与读写器之间或标签与其他 RFID 设备之间的通信数据。而且，由于从读写器到标签的前向信道具有较大的覆盖范围，因而它比从标签到读写器的后向信道更不安全。因此，射频通信层的通信数据的机密性也更为重要。

2）完整性

完整性是指保护射频通信模块的通信数据不允许被未授权修改。攻击者可以利用射频通信模块无线网络固有的脆弱性来篡改或重放信息，来破坏读写器与标签之间的正常通信，因此，需要运用加密、哈希散列和 CRC 校验等措施，来保证通信数据的完整性。

3）可用性

可用性是指保护通信信道能够正常通信。射频信号很容易受到干扰，恶意攻击者可能通过干扰广播、阻塞信道等方法来破坏射频通信信道，因此需要保证射频通信层的可用性。

4）可审计性

可审计性是指保证射频通信模块可以被监测、追踪和审计。

4.1.6 针对 RFID 系统的常见攻击方法

如前所述，RFID 系统一般由电子标签、天线、读写器、中间件、应用软件等部分组成。对于攻击者来说，这几个部分都有可能成为攻击的目标。

1. 针对标签和读写器的攻击

针对标签和读写器的常见的攻击方法，主要包括窃听、略读、克隆、重放、追踪、扰乱等。

1）窃听

RFID 系统通过无线电传递信息，读写器与标签之间的通信内容可以被窃听到。窃听是一种特殊的攻击行为，它可以远程实施，但发现却很困难，因为窃听是一个隐藏的行为，它不会产生任何信号。当敏感消息在信道内传输时，窃听攻击就构成一个严重的威胁。例如，将一个天线安装在 RFID 信用卡读写器附近，读写器与 RFID 信用卡之间的无线电信号有可能被捕获并翻译成可被人识别的形式。如果被捕获的是持卡人姓名、完整的信用卡号码、信用卡失效日期、信用卡类型、软件版本、支持的通信协议等重要信息，就会给持卡人带来经济损失。

攻击者通过窃听获取非公开的内部或机密的信息后，既可以利用这些信息，也可以出售这些信息谋取利益，或者公开这些信息使 RFID 系统处于被动状态，或者保存这些信息以备将来使用。

2）略读

略读是指在标签所有者不知情和没有得到所有者同意的情况下读取存储在 RFID 标签中的数据。它通过一个非法的读写器与标签交互来获取标签中存储的数据。由于某些标签在不需要认证的情况下会广播存储的内容，因此这种攻击行为有可能奏效。

略读攻击的一个典型例子是针对电子护照的攻击。电子护照中包含敏感信息，现有的强制被动认证机制要求使用数字签名，读写器能够读取来自电子护照中的数据。然而，由于读写器不需要被认证，标签会不加判断地进行回答。如果数字签名并没有与护照中的特定数据相关联，仅仅支持被动认证，那么拥有读写器的攻击者就能够获得护照持有人的姓名、性别、出生日期、护照号码甚至面部照片等敏感信息。

3）克隆

克隆就是攻击者非法地复制标签，并用复制的标签冒充合法的标签。

对于信用卡、电子车票等具有高安全性应用的支付系统，在设计 RFID 系统时，应当考虑实际的需求，选择具有加密功能的系统，如果忽视了加密过程，攻击者将有可能使用克隆的假冒标签而获取未经许可的服务，产生非常严重的安全隐患。

主动认证方法具有防克隆的特性，这种方法使用公钥加密，它依靠电子标签提供的私钥来工作：标签随机产生一个现时数据（nonce），并且用自己的私钥对其进行数字签名，然后将它发送给读写器，读写器利用标签中携带的与私钥配对的公钥来验证该签名的正确性。

4）重放

重放攻击即攻击者复制通信双方之间的一串信息流，并且重放给其中某一方或者双方。重放攻击是针对安全协议的攻击，可以欺骗通信参与者误认为攻击者已经成功地完成了认证。这种攻击对加密通信仍然可行，因为信息只是通过快速通信信道进行重放，而不需要知道其内容。

避免重放攻击的方法包括使用时间同步、递增的序列号或者现时数据等。但是，在 RFID 系统中，时间同步是不可行的，因为被动的 RFID 标签没有电源，不使用时钟；递增的序列号对不关心跟踪的 RFID 应用是一种可行的方案；对 RFID 标签来说，使用现时数据也是一种合适的方案。

5）追踪

攻击者有可能利用 RFID 标签上的信息，对 RFID 携带者进行跟踪，从而获取携带者所在的地理位置，即地址隐私信息。

6）扰乱

攻击者可以发射干扰信号，从而使系统陷入混乱状态，使 RFID 系统无法正常运行。这种攻击通过一个干扰设备广播无线电干扰信号来实施攻击，阻止 RFID 读写器与标签之间的正常通信，从而导致系统无法正常工作。

2．针对应用软件和后台数据库的攻击

针对应用软件和后台数据库的常见的攻击方法，主要包括标签伪造与复制、对象名字解析服务攻击和病毒攻击等。

1）标签伪造与复制

尽管伪造电子标签很困难，但在某些场合中，电子标签有可能被复制。这与信用卡被不

法分子复制并在多个地点同时被使用的情况很类似。由于复制的标签很难在使用时被区分出来，因此，在应用系统设计时应考虑到这种可能的安全隐患，并能防范这种非法复制标签的攻击行为。

2）对象名字解析服务攻击

对象名字解析服务（Object Name Service，ONS）是一种分布式目录服务，为请求关于EPC的信息提供路由。当一个RFID标签被制造成带有EPC编码时，EPC编码就被注册到ONS系统中。当RFID标签被贴在产品上时，EPC编码就成了产品的一部分，跟随供应链一起移动。

ONS在技术与功能上都与域名服务（Domain Name Service，DNS）非常类似。一个开放式的、全球性的追踪物品的网络需要特殊的网络结构。因为除了将EPC编码存储在标签中外，还需要一些将EPC码与相应商品信息进行匹配的方法。这个功能就由对象名解析服务（ONS）来实现，它是一个自动的网络服务系统，类似于域名解析服务（DNS），DNS是将一台计算机定位到万维网上的某一具体地点的服务。

当一个读写器读取一个EPC标签的信息时，EPC码就传递给了后台数据库系统。后台数据库系统然后再在局域网或因特网上利用ONS对象名解析服务找到这个产品信息所存储的位置。ONS给后台数据库系统指明了存储这个产品的索引信息的服务器，因此就能够在后台数据库系统中找到这个索引信息，并且将这个索引信息对应的这个产品的详细信息传递过来，从而实现供应链的管理。

ONS面临的主要安全威胁如下：

（1）包拦截：拦截携带ONS信息的IP数据包。

（2）查询预测：操纵ONS协议的查询/回答方案。

（3）缓存中毒：注入被操纵的信息进入ONS缓存。

（4）DoS攻击：即拒绝服务攻击，透过大量合法或伪造的请求占用大量网络以及器材资源，以达到瘫痪网络以及系统的目的。

3）病毒攻击

RFID电子标签的存储器中包括了许多重要信息，数据的长度从几个字节到几千个字节。其中存储额外信息的空间有可能被重写。由于标签传送的信息被绝对信任，因此带来了安全隐患。

（1）缓存溢出。

这是应用软件常见的安全隐患之一。在C++语言中，由于输入的长度不被检查，因此攻击者可以引入超出正常长度的输入，甚至超出变量的缓存区域。当程序控制代码位于邻近数据缓存的存储区域时，缓存溢出有可能会导致程序执行某段恶意代码。

（2）编码植入。

攻击者可能使用某种脚本语言（CGI、Java、Perl等）将恶意代码注入一个应用软件中。带有注入脚本语言代码的电子标签可能会执行这些代码，从而使RFID系统受到攻击。

（3）结构化查询语言注入。

指在数据库中执行非授权的结构化查询（SQL查询）。这类攻击的主要目的是分析数据库结构、检索数据、进行非授权的修改或删除。RFID标签有可能被注入包含SQL攻击的恶意代码。

4.1.7 RFID 系统的安全机制

RFID 系统的安全机制可以分为三大类：物理安全机制、密码安全机制以及两者相结合的安全机制。

1. 物理安全机制

物理安全机制通常用于低成本标签中，因为这些标签难以采用复杂的密码机制来实现与读写器之间的安全通信。物理机制主要包括五大类：杀死命令机制、休眠机制、阻塞机制、静电屏蔽和主动干扰等。

1）杀死命令机制

杀死(Kill)命令机制是解决信息泄露的一种简单方法。这种方法是从物理上毁坏标签，一旦对电子标签下达了杀死(Kill)命令，电子标签便处于失效状态，不能被再次使用。执行了杀死命令之后，标签便终止了其生命，不能再发送或接收数据，这是一个不可逆的操作。为了防止标签被非法杀死，通常都需要进行口令认证。

在实际应用中，当超市结账时，可以使用 Kill 命令杀死粘贴在商品上的电子标签，以表明该商品已经出售。然而，在商品出售之后，还有可能遇到反向物流的问题，例如退货、维修、召回等，如果电子标签已经被杀死，RFID 标签就不可能被再次利用。为此，IBM 公司开发出一种的可裁剪标签。结账时可以将 RFID 标签的天线刮除，从而缩短标签可阅读的距离，使标签不能被远距离读取。再次使用该标签时，虽然天线已经不能再使用，但是读写器仍能在近距离读取标签。这样，当消费者需要退货时，仍可以从 RFID 标签中读出相关的信息。

2）休眠机制

休眠(Sleeping)机制是使得电子标签进入睡眠状态，而不是死亡。处于睡眠状态的电子标签，以后还可以通过唤醒命令将其唤醒。

采用休眠机制，休眠中的 RFID 标签虽然不再响应读写命令，但是如果收到唤醒命令并且口令正确，标签就可以被唤醒，重新激活，就能够再次投入使用。

对于某些商品，消费者往往希望在保持隐私的前提下，还能够继续读取和利用标签中的信息。例如，粘贴在食品上的休眠中的标签并未失效，当它被唤醒后，安装在家用智能电冰箱中的 RFID 读写器可以自动识别 RFID 标签中存储的食品的类别、数量、有效期等相关信息，如果食品即将到期或者已经过期，就会提醒主人取出过期的食品。

3）阻塞机制

阻塞(Blocking)机制通过标签中特定隐私位来限制读写器对电子标签的访问。如果隐私位为 0，表示标签是公开的，可以接受读写器的访问；如果隐私位为 1，则表示标签是保密的，不能够被读写器访问。从工厂生产出的某件产品贴上 RFID 标签起一直到该产品出售之前，即该产品在仓库、运输途中、超级市场的货架的时候，其隐私位设置为 0。此时，任何读写器都可以扫描产品的 RFID 标签。当消费者购买了贴有标签的该产品时，销售终端设备将隐私位设置为 1，从而限制读写器对电子标签的访问。

4）静电屏蔽

静电屏蔽(Electrostatic Shielding)也称为法拉第网罩(Faraday Cage)屏蔽。由于无线

电波会被金属材料做成的屏蔽网屏蔽，因此可以将贴有RFID标签的商品放入由金属网罩或金属箔片组成的容器中，从而阻止标签与非法读写器之间的通信。然而，由于每一件商品都需要一个网罩，因此静电屏蔽会增加成本。

5）主动干扰

主动干扰法是标签用户通过一个设备主动广播无线电信号用于阻止或破坏附近的非法RFID读写器的窃听攻击。但是这一方法也可能干扰附近的合法RFID系统的正常读写，甚至会阻塞附近的无线电信号，对其他通信系统造成干扰。

2. 密码安全机制

RFID系统的密码安全机制是指利用各种成熟的加密算法和安全机制，来设计和实现符合RFID系统的安全需求。近年来，研究者们提出了很多低成本的安全认证协议，例如hash-lock（哈希锁）协议、随机化hash-lock（随机化哈希锁）协议、hash-chain（哈希链）协议、Hash函数构造算法、基于矩阵密钥的认证协议、数字图书馆协议等。以下将对这些认证协议作简要介绍。

1）哈希锁（Hash-Lock）协议

哈希锁协议最早由Sarma等学者提出，它是一种基于单向哈希（Hash）函数的加密机制。每一个具有哈希锁的标签中，都有一个哈希函数，并存储一个临时的标识metaID。基于哈希锁协议的标签，可以工作在锁定或非锁定两种状态。当具有哈希锁的标签处于锁定状态时，针对读写器对其进行查询的请求，仅仅回复标识metaID；只有标签处于非锁定状态时，针对读写器对其进行查询的请求，标签才会向读写器提供除了标识metaID以外的完整的信息。

基于哈希锁协议的认证过程如图4-2所示。

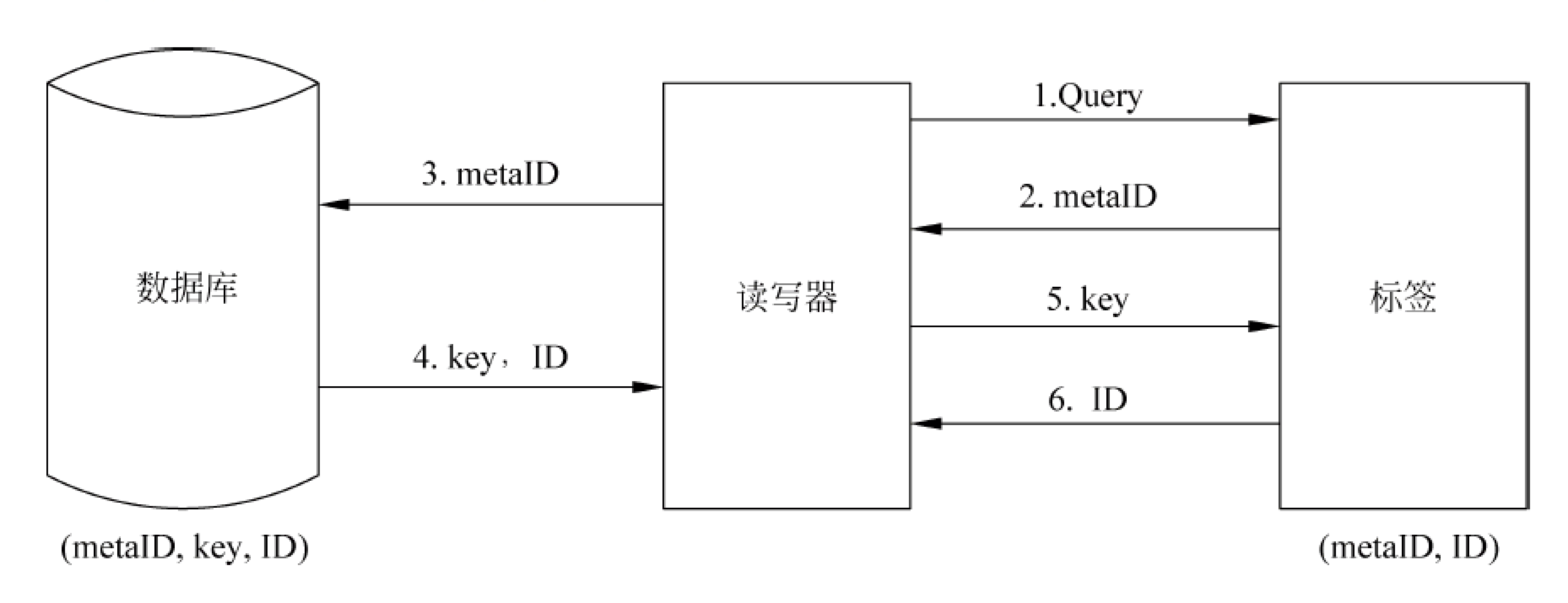


图4-2　基于哈希锁协议的认证过程

基于哈希锁协议的认证过程的步骤如下：

（1）读写器向标签发送认证请求Query，即向标签问询其标识。

（2）标签将metaID发送给读写器。

（3）读写器将metaID转发到后台数据库。

（4）后台数据库查询自己的数据，如果能找到与metaID匹配的项，则将该项的（key，ID）发送给读写器，其中ID为待认证标签的标识；否则，返回给读写器认证失败信息。

（5）读写器将从后台数据库接收的解锁信息key发送给标签。

(6) 标签验证 metaID=Hash(key)是否成立，如果成立，则对读写器的认证通过，标签将其 ID 发送给读写器；否则认证失败。

(7) 读写器比较从标签接收到的 ID 是否与后台数据库发送过来的 ID 一致，如果一致，则对标签的认证通过；否则认证失败。

哈希锁协议的优点是标签运算量小，数据库查询快，并且可以实现标签对读写器的认证。但是其安全漏洞也比较多：没有 ID 动态刷新机制，且 metaID 保持不变，并以明文传送，因此标签很容易被跟踪、窃听和克隆；此外，重放攻击、中间人攻击、拒绝服务攻击等均可实施。由于存在这些漏洞，因此其安全性不高，不能完全达到保护 ID 不产生泄漏的目标。

2) 随机哈希锁(Random Hash-Lock)协议

随机哈希锁协议最早由 Weis 等学者提出。它将原来的哈希锁协议加以改进，把原来取固定数值的标识 metaID 进行加密，使之变成随机的数值，不停地变化，从而避免攻击者的追踪。标签中除了 Hash 函数以外，还嵌入了伪随机数发生器，在后台数据库存储所有标签的 ID，它采用了基于随机数的询问-应答机制。即由认证方询问，被认证方回答。如果回答正确，则说明被认证方的身份合法，可以通过认证；否则，如果回答错误，则说明被认证方身份有误，无法通过认证。

基于随机哈希锁协议的认证过程如图 4-3 所示。

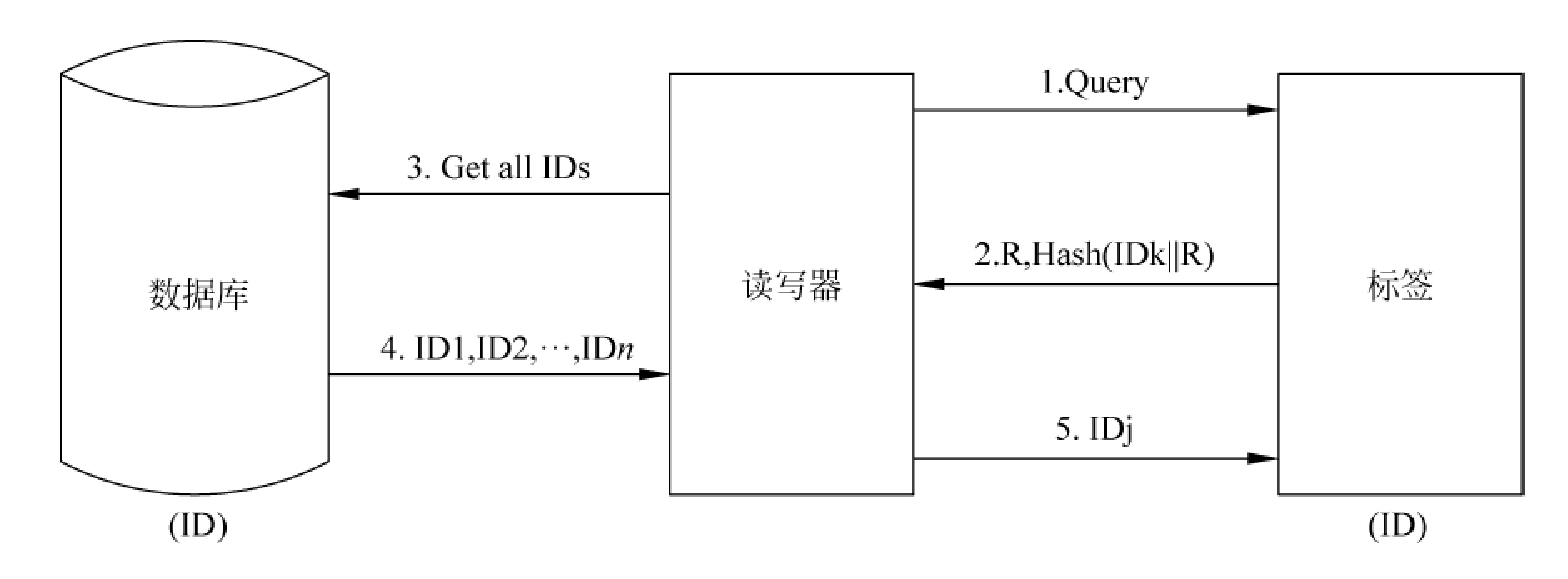


图 4-3 基于随机哈希锁协议的认证过程

基于随机哈希锁协议的认证步骤如下：

(1) 读写器向标签发送认证请求 Query，即向标签询问其标识。

(2) 标签生成一个随机数 R，计算 Hash(IDk||R)，其中 IDk 为标签的标识。标签将(R，Hash(IDk||R))发送给读写器。

(3) 读写器向后台数据库请求获得所有标签的标识。

(4) 后台数据库将自己数据库中的所有标签的标识(ID1，ID2，…，IDn)发送给读写器。

(5) 读写器检查是否有某个 IDj($1\leqslant j\leqslant n$)，使得 Hash(ID||R)成立；如果有，则对标签的认证通过，并且将这个 ID 发送给读写器；否则认证失败。

(6) 标签验证。检查 IDj 与 IDk 是否相同，如果相同则对读写器的认证通过，否则认证失败。

随机哈希锁协议也采取双向认证，虽然消息 2 随机变化，但是在认证过程中仍然存在安全漏洞：认证通过后的标签标识 IDj 仍以明文的形式在不安全信道传送，攻击者仍然可以对标签进行追踪。并且，一旦获得了标签的标识 IDj，攻击者就可以对标签进行假冒。因

此，随机哈希锁协议也并不安全。此外，每一次标签认证时，后台数据库都需要将所有标签的标识发送给读写器，两者之间的数据通信量很大，所以效率比较低。

3）哈希链（Hash-Chain）协议

哈希链协议是一种共享秘密的“询问-应答”协议。当不同的读写器发起认证请求时，如果读写器中的 Hash 函数不同，则标签的应答就不同，其认证过程如图 4-4 所示。

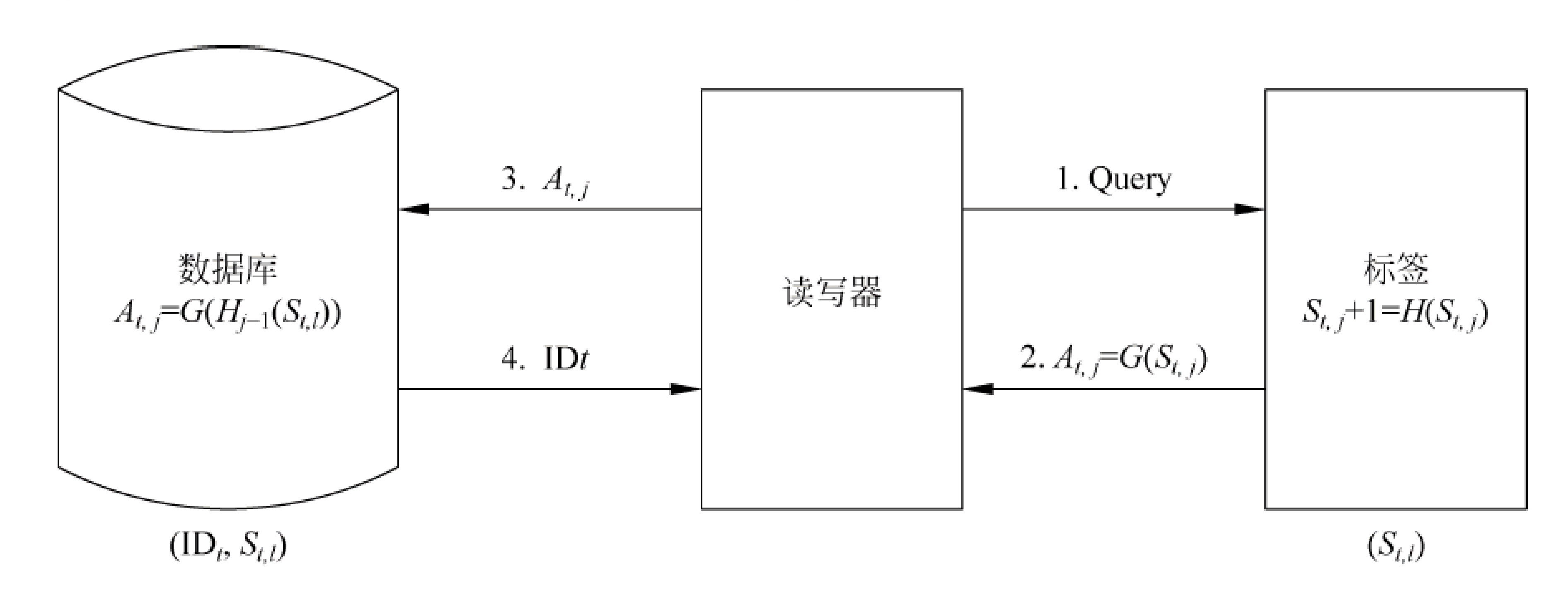


图 4-4 基于哈希链协议的认证过程

在系统运行之前，电子标签和后台数据库首先要共享一个初始密钥 $S_{t,j}$，标签与读写器之间执行第 j 次 Hash-Chain 协议的过程如下：

（1）读写器向标签发送认证请求 Query，即向标签问询其标识。

（2）标签使用当前的密钥 $S_{t,j}$ 计算 $A_{t,j}=G(S_{t,j})$（注：G 也是一个安全的 Hash 函数），并更新其密钥为 $S_{t,j+1}=\text{Hash}(S_{t,j})$，标签将 $A_{t,j}$ 发送给读写器。

（3）读写器将 $A_{t,j}$ 转发给后台数据库。

（4）后台数据库针对所有的标签数据项，查找并计算是否存在某个 IDt（$1\leqslant t\leqslant n$）和是否存在某一个 j（$1\leqslant j\leqslant m$），其中 m 为系统预先设定的最大链长度，使得 $A_{t,j}=G(H^{j-1}(S_{t,1}))$成立，如果有，则认证通过，并将 ID$t$ 发送给标签；否则，认证失败。

由于 G 函数是单向函数，攻击者观察到的 $A_{t,j}$ 与 $A_{t,j+1}$ 是不可关联的，因此哈希链协议实现了不可追踪性。但是哈希链协议仍然容易受到假冒和重传攻击，只要攻击者截获某个 $A_{t,j}$，就可以进行重传攻击，伪装成合法的标签。每次认证时，后台都要对每个标签进行 j 次 Hash 计算，运算量比较大。此外，协议至少需要两个 Hash 函数，增加了硬件的成本。

4）哈希函数构造算法

哈希函数构造算法最早由中国学者杨骅等人提出，其实现流程如图 4-5 所示。

哈希函数构造算法最终要生成可供 RFID 进行安全认证的 16 位哈希（Hash）值。算法共选取 4 个映射，分别为帐篷映射、立方映射、锯齿映射和虫口映射。将每两个映射作为一组，共可以组成 6 组。映射组合的选择由读写器通过命令参数传递给标签。读写器发送命令给标签。标签根据读写器命令中的参数，在存储区域选择数据作为计算 Hash 值的初值，计算出 Hash 值回传给读写器。在 RFID 系统中，可以利用标签的 ID 号或其他存储内容作为初始的消息数。把 N 个初值元素平分为 2 组，每组元素选择不同映射各迭代 $m/2$ 次，交换映射后再迭代 $m/2$ 次，每个元素共迭代了 m 次。将奇数位置上的数组元素（第 1，3，5…数组元素）进行按位异或运算，经过 $N/2-1$ 次异或运算，得到 n 位数值；同理，偶数位上的数组元素（第 2，4，6…数组元素）也可以得到 n 位数值，将两个 n 位数值分别映射为 8bit 数

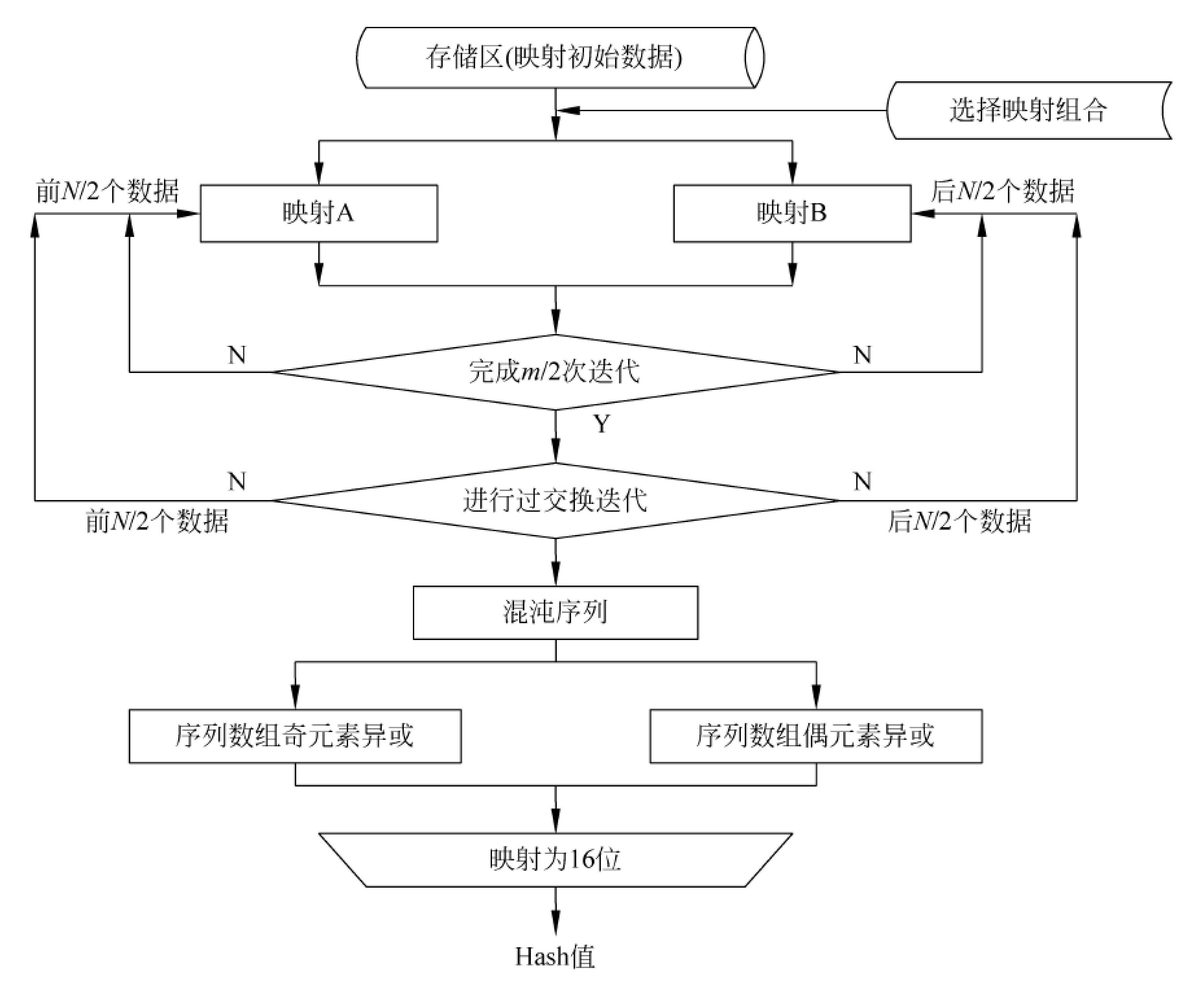


图 4-5 Hash 函数构造算法流程

值，最终组合成 16 位的 Hash 值。

哈希函数构造算法基于混沌映射，通过 4 个混沌映射构造出 6 种组合，RFID 系统可以灵活选择映射组合，从而构造安全认证需要的 Hash 值。该算法实现了较低的复杂度，可以在芯片面积、功耗、速度方面满足 RFID 标签芯片要求；同时由于混沌系统固有的特点，使算法对初值有高度敏感性，具有很好的单向 Hash 函数性能，满足了 RFID 系统的安全性要求。

5）基于矩阵密钥的认证协议

基于矩阵密钥的认证协议最早由中国学者裴友林等人提出。该协议的特点是以双矩阵作为密钥。当进行加密时，由明文与密钥矩阵相乘得到密文；当解密时，则由密文与密钥逆矩阵相乘来还原明文。其算法实现流程如图 4-6 所示。

在基于双矩阵密钥的 RFID 双向认证协议中，每个标签的认证过程中需要使用 2 个矩阵密钥，记为 $\boldsymbol{K}_1$ 和 $\boldsymbol{K}_2$，$\boldsymbol{K}_1$ 和 $\boldsymbol{K}_2$ 是 n 阶可逆方阵。$\boldsymbol{K}_1'$，$\boldsymbol{K}_2'$分别是其逆方阵。标签中存储密值 $\boldsymbol{S}$ 和 2 个矩阵 $\boldsymbol{K}_1$ 及 $\boldsymbol{K}_2'$。密值 $\boldsymbol{S}$ 是长度为 q 的向量，$q=m\times n$，m 是正整数。

后台数据库为每个标签存储($\boldsymbol{X}$，$\boldsymbol{S}$，$\boldsymbol{K}_1'$，$\boldsymbol{K}_2'$)这样的记录，$\boldsymbol{X}$ 表示该标签记录在数据库中的索引。$\boldsymbol{X}$ 是长度为 $\boldsymbol{q}$ 的向量，其值可通过对 $\boldsymbol{K}1$ 和 $\boldsymbol{S}$ 进行下列运算得到：将 $\boldsymbol{S}$ 划分成 m 个长度为 n 的向量，$\boldsymbol{S}=(S_1,S_2,\cdots,S_i,\cdots,S_m)$，则 $\boldsymbol{X}=(X_1,X_2,\cdots,X_i,\cdots,X_m)$，其中 $\boldsymbol{S}_i$ 和 $\boldsymbol{X}_i$ 是长度为 n 的向量且 $\boldsymbol{X}_i=\boldsymbol{K}_1\boldsymbol{S}_i(1\leqslant i\leqslant m)$。

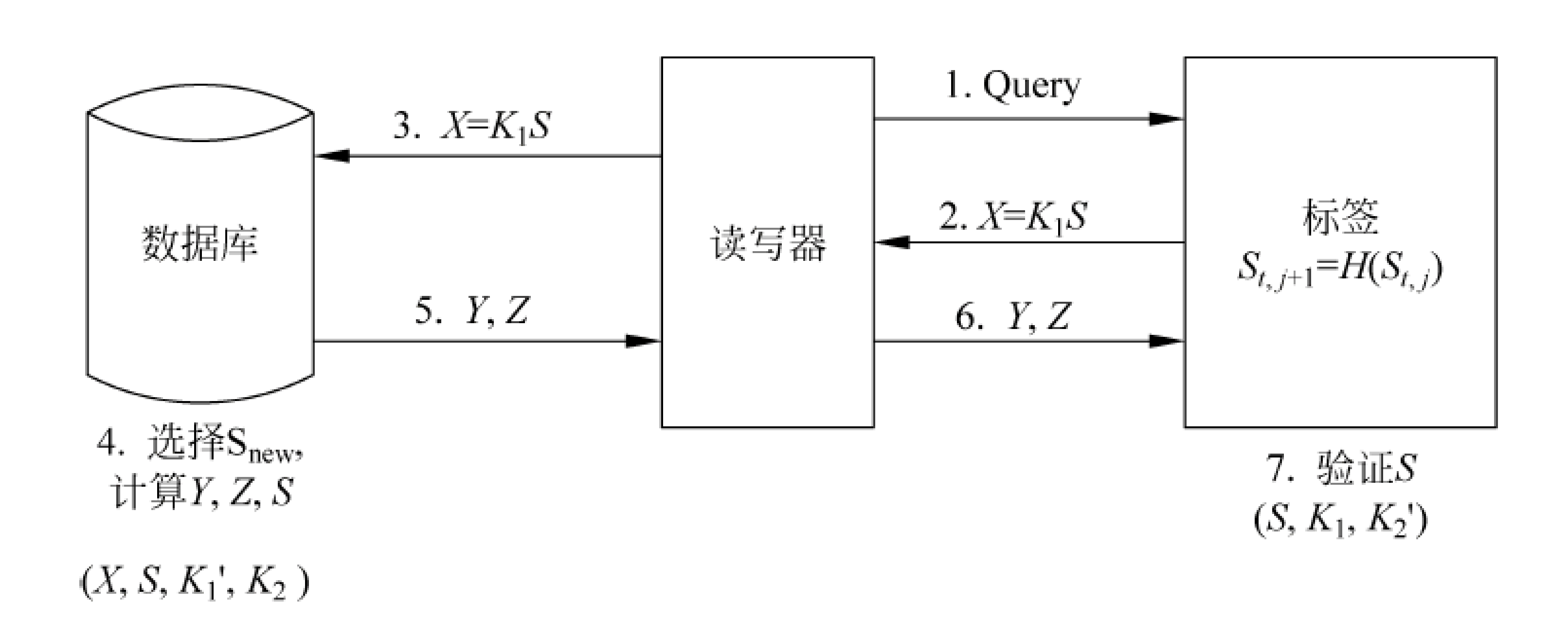


图 4-6　基于矩阵密钥的认证协议

基于矩阵密钥的认证协议的认证步骤如下：

初始化时，为每个标签随机选择可逆方阵 $\boldsymbol{K}_1$ 和 $\boldsymbol{K}_2$。选择唯一的 $\boldsymbol{X}$，并根据 $\boldsymbol{X}$ 值，计算 $\boldsymbol{K}_1'\boldsymbol{X}$，得到密值 $\boldsymbol{S}$。将这些信息存储进标签和数据库。

(1) 读写器向标签发送 Query 认证请求。

(2) 标签计算 $\boldsymbol{X}=\boldsymbol{K}_1\boldsymbol{S}$，将 $\boldsymbol{X}$ 发送给读写器。

(3) 读写器将 $\boldsymbol{X}$ 转发给后台数据库。

(4) 后台数据库搜索数据，找到相应的 $\boldsymbol{X}$。计算 $\boldsymbol{K}'\boldsymbol{X}$，并验证此值与 $\boldsymbol{S}$ 是否相同。如果不同，则认证不通过；如果相同，则选择使 $\boldsymbol{X}_{new}$ 唯一的 $\boldsymbol{S}_{new}$，计算 $\boldsymbol{Y}=\boldsymbol{K}_2\boldsymbol{S}$，$\boldsymbol{Z}=\boldsymbol{K}_2\boldsymbol{S}_{new}$，更新 $\boldsymbol{S}$。将 $\boldsymbol{Y}$，$\boldsymbol{Z}$ 发送给读写器。

(5) 读写器将 $\boldsymbol{Y}$，$\boldsymbol{Z}$ 转发给标签。

(6) 标签计算 $\boldsymbol{K}_2'\boldsymbol{Y}$，验证此值是否与 $\boldsymbol{S}$ 相同。如果不同，认证不通过；相同，计算 $\boldsymbol{K}_2'\boldsymbol{Z}$，并将 $\boldsymbol{S}$ 更新为此值。

基于密钥矩阵的安全认证协议，在保证标签隐私安全的前提下，提高了认证的执行效率及应用成本。但此协议还有不足之处，标签中存储信息量较大。此外，需要做到标签中信息和后台数据库的同步更新，不适用于分布式环境。

6) 改进型 David 数字图书馆协议

改进型 David 数字图书馆协议最早由中国学者郭维等人提出，其工作原理如图 4-7 所示。

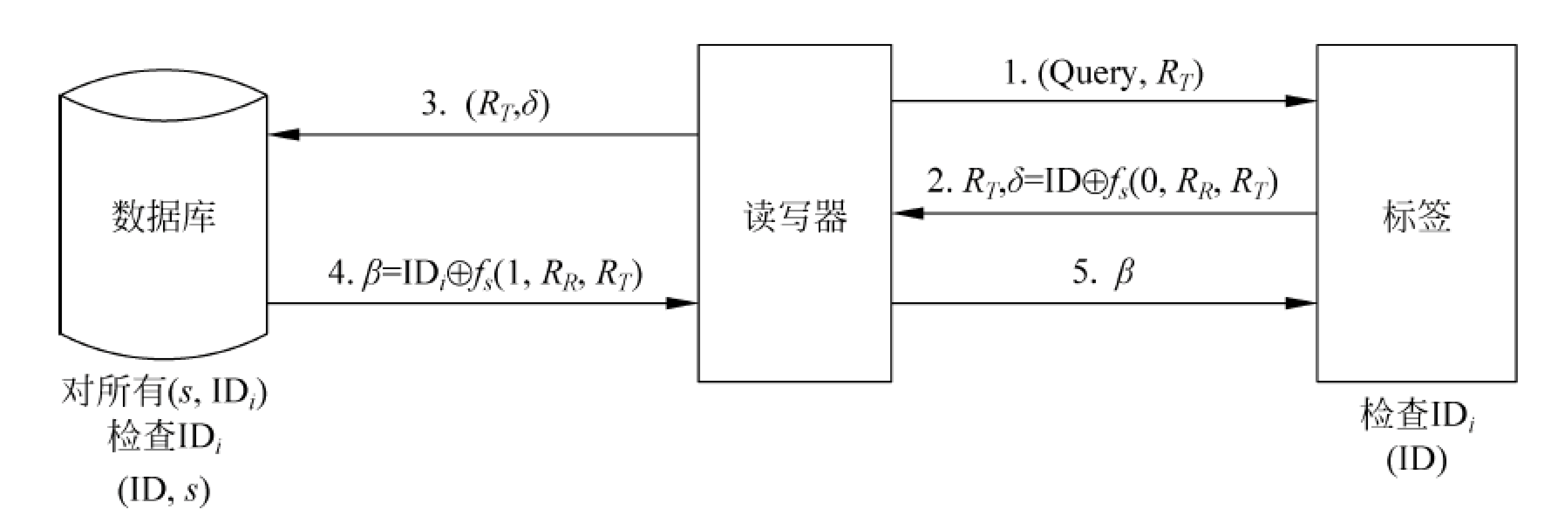


图 4-7　改进型 David 数字图书馆协议

系统运行之前，后台数据库和每一个标签之间需要预先共享一个秘密值 s。标签中有一个 R_T 值，用来存放一个模拟的随机数。其中 f_s 是带密钥的 Hash 函数，f_s^L 和 f_s^R 分别表

示其运算结果的左部分和右部分，即将 Hash 值一分为二。该协议的执行过程如下：

(1) 读写器生成一个秘密随机数 R_T，并向标签发送(Query，R_T)认证请求。

(2) 标签使用自己的 ID、秘密值 s 和预存的模拟随机数 R_R，计算 $\delta=\text{ID}\oplus f_s^L(0,R_R,R_T)$，标签将($R_T$，$\delta$)发送给读写器，然后刷新 R_R 为 $R_R=f_s^R(0,R_R,R_T)$。

(3) 读写器将(R_T，δ)转发给后台数据库。

(4) 后台数据库查询自己的数据库，如果找到某个 $\text{ID}_j(1\leqslant j\leqslant n)$，使得 $\delta=\text{ID}_j\oplus f_s^L(0,R_R,R_T)$成立；则认证通过，并计算 $\beta=\text{ID}_j\oplus f_s^L(1,R_R,R_T)$，然后将 β 发送给读写器；否则返回给读写器认证失败信息。

(5) 读写器将 β 转发送给标签。

(6) 标签验证 $\text{ID}=\beta\oplus f_s^L(1,R_R,R_T)$是否成立。如果成立，则认证通过；否则认证失败。

由于 R_T 是由读写器生成的，故具有随机性，而 $R_R=f_s^R(0,R_R,R_T)$，故 R_R 也具有随机性，攻击者无法事先获得 R_R。这是该协议的关键，将原来由标签中专门设置伪随机数函数来生成伪随机数转为直接由 Hash 函数来生成的伪随机数 R_R，从而减少了标签中用来实现伪随机数函数的电路模块，大大地降低了成本。

由于 $\delta=\text{ID}\oplus f_s^L(0,R_R,R_T)$中含有不可预知的随机数 R_R，故每次通信时，δ 都具有随机性，所以无法跟踪，保护了隐私性。

4.2 无线传感器网络安全

4.2.1 无线传感器网络概述

无线传感器网络(Wireless Sensor Networks，WSN)是由部署在监测区域内大量的廉价微型传感器结点组成，并通过无线通信方式形成的一个多跳的、自组织的网络系统，其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息，并发送给观察者。传感器、感知对象和观察者构成了无线传感器网络的三个要素。

微机电系统(Micro-Electro-Mechanism System，MEMS)、片上系统(System On Chip，SOC)、无线通信和低功耗嵌入式技术的飞速发展，孕育了无线传感器网络。无线传感器网络以其低功耗、低成本、分布式和自组织的特点带来了信息感知领域的一场变革。

许多学者认为，无线传感器网络技术的重要性可与因特网相媲美。正如互联网使得计算机能够访问各种数字信息而可以不管其保存在什么地方一样，传感器网络将能扩展人们与现实世界进行远程交互的能力。它甚至被人们称为一种全新类型的计算机系统，这是因为它具有区别于过去硬件的、可以到处散布的特点和集体分析能力。

无线传感器网络具有众多不同类型的传感器，可以探测包括地震、电磁、温度、湿度、噪声、光强度、压力、土壤成分、移动物体的大小、速度和方向等周边环境中多种多样的物理量和化学量。基于 MEMS 的微传感技术和无线网络技术，为无线传感器网络赋予了广阔的应用前景。这些潜在的应用领域可以归纳为军事、航空、反恐、防爆、救灾、环境、医疗、保健、家居、工业、商业等领域。

4.2.2 无线传感器网络的发展历程

到目前为止,无线传感器网络的发展历程共经历了三个阶段:传感器→无线传感器→无线传感器网络。

第一阶段:传感器网络最早可以追溯至越战时期美国军方使用的传感器系统。当年,美越双方在密林覆盖的“胡志明小道”进行了一场血腥的较量,“胡志明小道”是越南部队向南方游击队输送军事物资的秘密通道,美军对其进行了狂轰滥炸,但是效果不大。后来,美军投放了2万多个“热带树”传感器。“热带树”实际上是由震动和声响传感器组成的系统,它由飞机投放,落地后插入泥土中,只露出伪装成树枝的无线电天线,因而被称为“热带树”。一旦越方的车队经过,传感器就能探测出目标产生的震动和声响信息,并自动发送到指挥中心,引导美方的军机针对目标准确地展开轰炸。在这场战争中,美军总共炸毁或炸坏了越南部队4.6万辆卡车。

第二阶段:位于20世纪80～90年代,主要是美军研制的分布式传感器网络系统、海军协同交战能力系统、远程战场传感器系统等。这种现代微型化的传感器同时具备感知能力、计算能力和通信能力。在1999年,美国《商业周刊》(Businessweek)杂志将传感器网络列为21世纪最具影响的21项技术之一。

第三阶段:从21世纪开始至今,也就是美国“9・11”事件之后。这个阶段的传感器网络技术特点在于网络传输自组织、结点设计低功耗。除了应用于反恐活动以外,在其他领域也获得了很好的应用,所以2002年美国国家重点实验室——橡树岭实验室提出了“网络就是传感器”的论断。

在现代意义上的无线传感器网络研究及其应用方面,我国与发达国家几乎同步启动,它已经成为我国信息领域位居世界前列的少数方向之一。在2006年我国发布的《国家中长期科学与技术发展规划纲要》中,为信息技术确定了三个前沿方向,其中有两项就与无线传感器网络直接相关,这就是智能感知和自组网技术。当然,传感器网络的发展也是符合计算设备的演化规律的。

4.2.3 无线传感器网络的系统结构

无线传感器网络系统通常包括无线传感器结点、网络协调器和中央控制器。大量无线传感器结点随机部署在监测区域内部或附近,这一过程可以通过飞机撒播、人工掩埋或火箭发射等方式实现。无线传感器能够通过自组织方式构成网络。传感器结点监测的数据沿着其他传感器结点逐跳地进行传输,在传输过程中监测数据可能被多个结点处理以提高处理效率,监测数据经过多跳后传输到汇聚结点,最后通过互联网或卫星到达中央控制点。用户通过中央控制点对传感器网络进行配置和管理,发布监测任务以及收集监测数据。典型的无线传感器网络的系统结构如图4-8所示。

在各种无线传感器网络中,传感器数据采集及传输常用的方式主要有周期性采样、事件驱动和存储与转发。实现其技术的网络拓扑结构也分为3种:星型网、网型网和混合网(星型网+网型网)。每一种拓扑网络结构都有其各自的优点和缺点,应当充分了解这些网络的特点,以满足各种不同应用的实际需求,如图4-9所示。

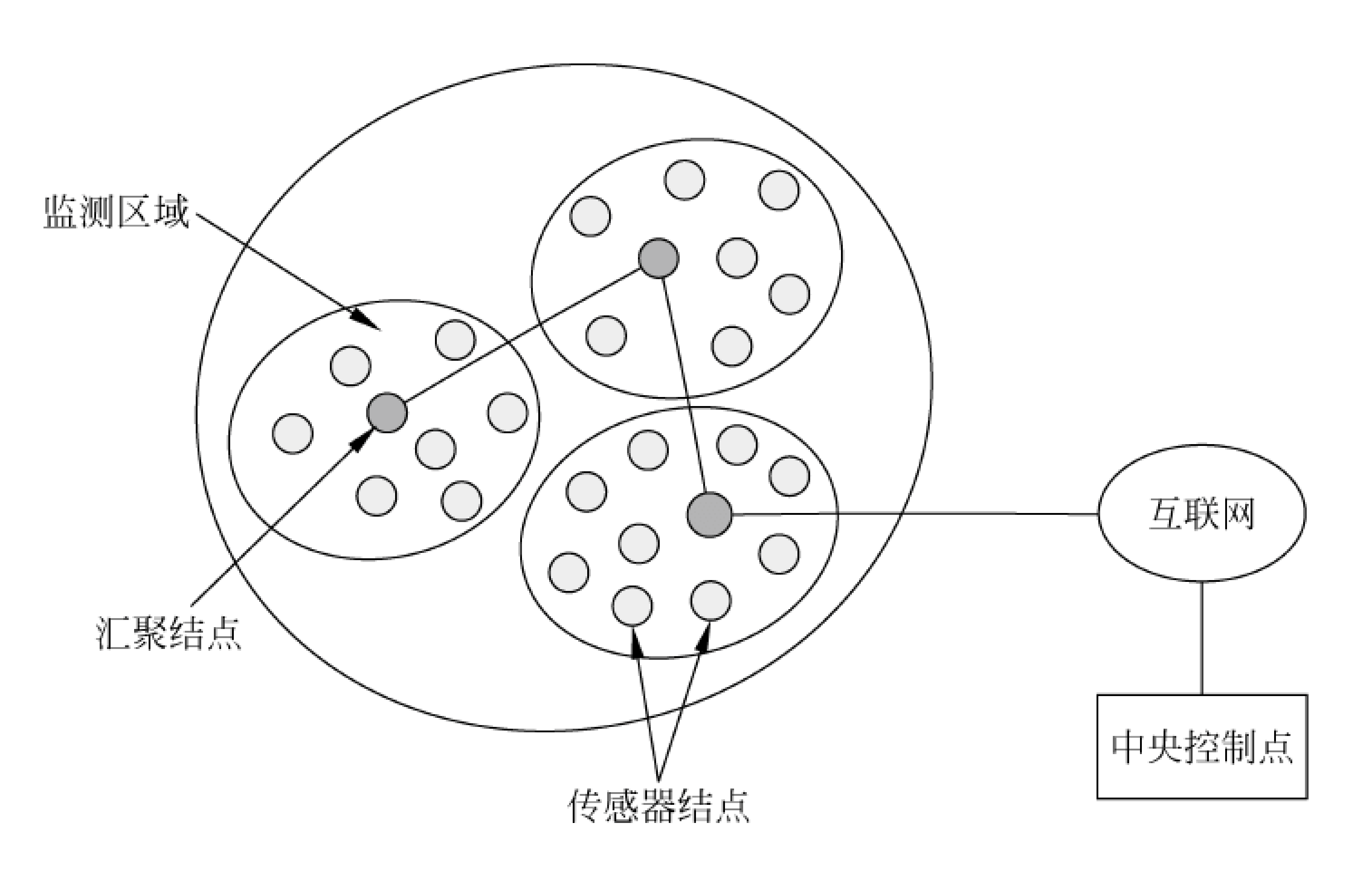


图 4-8　无线传感器网络的系统结构

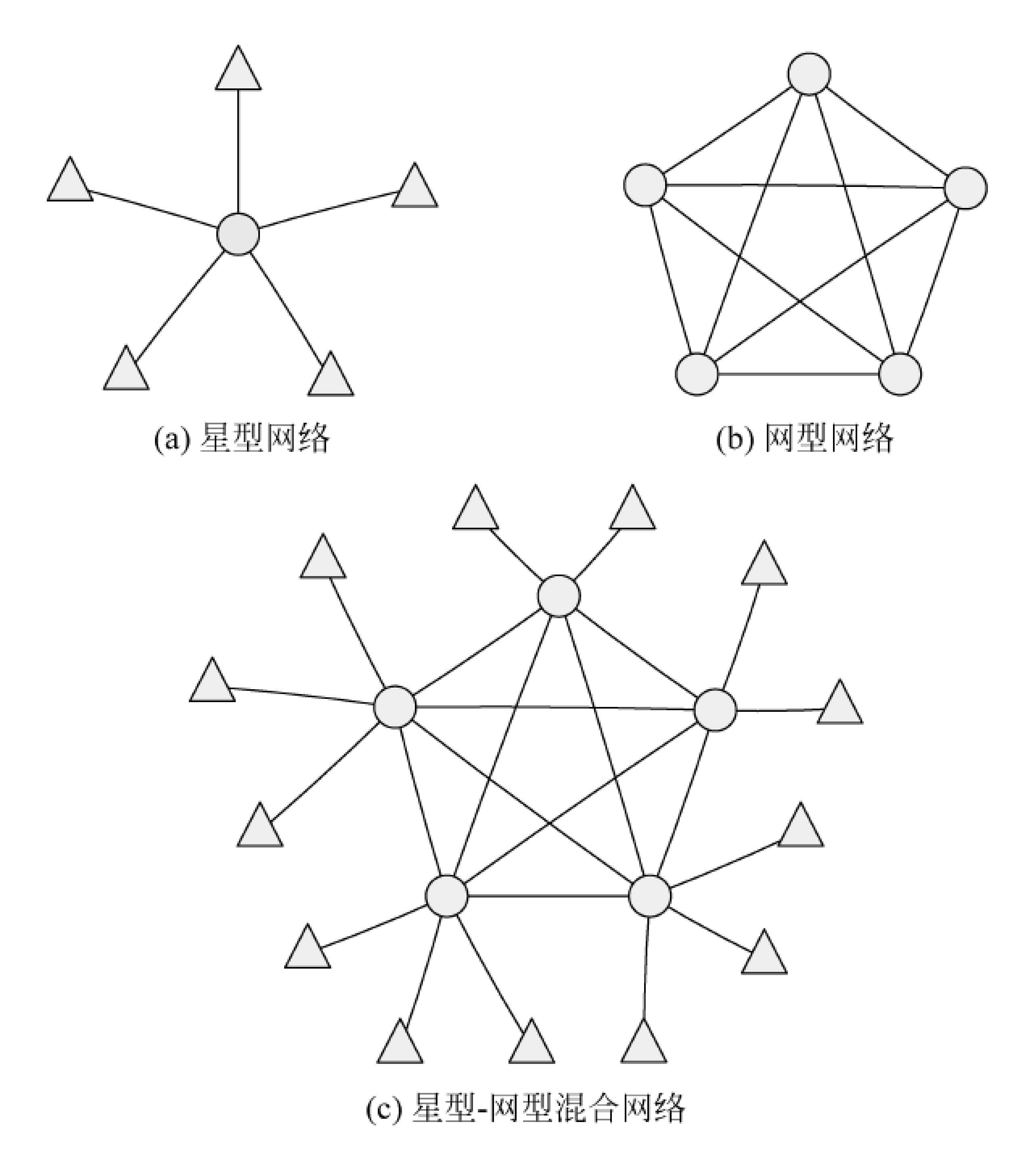


图 4-9　无线传感器网络拓扑结构

1. 星型无线传感器网络的拓扑结构

图 4-9(a)表示采用星型拓扑结构的无线传感器网络，其中心结点可以是 Wi-Fi 接入点、WiMAX 基站、蓝牙主设备或 ZigBee PAN 协调器，其作用与有线局域网中的交换机类似，采用不同的无线网络技术，其中心控制结点的功能也各有不同。星型拓扑结构是一种单跳系统，网络中所有无线传感器都与基站、网关或汇聚结点进行双向通信。基站可以是一台计算机、手机、PDA、专用控制设备、嵌入式网络服务器，或其他与高数据率设备通信的网关，

网络中各传感器结点基本相同。除了向各结点传输数据和命令外，基站还与互联网等更高层系统传输数据。各结点将基站作为一个中间点，相互之间并不传输数据或命令。在各种无线传感器网络中，星型网整体功耗最低，但结点与基站间的传输距离有限，通常 ISM 频段的传输距离约为 10～30 米。

2. 网型无线传感器网络的拓扑结构

图 4-9(b)表示采用网型拓扑结构的无线传感器网络。网型无线传感器网络也称为移动 Adhoc 网络，属于无线局域网或者无线城域网，网络中的结点可以移动，而且可以直接与相邻结点通信而不需要中心控制设备。因为结点可以随时进入或者离开网络，所以网型无线传感器网络的拓扑结构也在不停地变化。数据包从一个结点到另一个结点直至目的地的过程称为“跳”。网型无线传感器网络是一个多跳系统，其中所有无线传感器结点都相同，而且可以互相通信，经过其他结点与基站进行通信，传输数据和命令。由于网型网络的每一个传感器结点都有多条路径到达网关或其他结点，因此它的容错能力比较强。网型网络比星型网络的传输距离远得多，但功耗也更大，因为结点必须一直“监听”网络中某些路径上的信息和变化。

3. 混合型无线传感器网络的拓扑结构

采用混合型拓扑结构的无线传感器网络，兼具了星型网的简洁、低功耗和网型网的长传输距离和自愈性等优点，如图 4-9(c)所示。在混合网中，路由器和中继设备组成网型结构，而无线传感器结点则在它们附近呈星型分布。中继设备扩展了网络传输距离，同时提供了容错能力。由于无线传感器结点可以与多个路由器或中继设备通信，当某个路由器发生故障或某条无线链路出现错误时，网络可以与其他路由器进行自组网。

4.2.4　无线传感器网络的特点

1. 大规模

为了获取精确信息，在监测区域通常部署大量传感器结点，数量可能达到成千上万，甚至更多。传感器网络的大规模性包括两方面的含义：一方面是指传感器结点分布在很大的地理区域内，如在原始大森林采用无线传感器网络进行森林防火和环境监测，需要部署大量的传感器结点；另一方面是指传感器结点部署很密集，在面积较小的空间内，密集部署了大量的传感器结点。

无线传感器网络的大规模性具有如下优点：通过不同空间视角获得的信息具有更大的信噪比；通过分布式处理大量的采集信息能够提高监测的精确度，降低对单个结点传感器的精度要求；大量冗余结点的存在，使得系统具有很强的容错性能；大量结点能够增大覆盖的监测区域，减少洞穴或者盲区。

2. 自组织

在无线传感器网络应用中，通常情况下传感器结点被放置在没有基础结构的地方，传感器结点的位置不能预先精确设定，结点之间的相互邻居关系预先也不知道，如通过飞机播撒

大量传感器结点到面积广阔的原始森林中，或随意放置到人不可到达或危险的区域。这样就要求传感器结点具有自组织的能力，能够自动进行配置和管理，通过拓扑控制机制和网络协议自动形成转发监测数据的多跳无线网络系统。

在无线传感器网络使用过程中，部分传感器结点由于能量耗尽或环境因素造成失效，也有一些结点为了弥补失效结点、增加监测精度而补充到网络中，这样在传感器网络中结点的数量就会动态地增加或减少，从而使网络的拓扑结构也会随之动态地变化。传感器网络的自组织性要能够适应这种网络拓扑结构的动态变化。

3. 动态性

无线传感器网络的拓扑结构可能因为下列因素而改变：

(1) 环境因素或电能耗尽造成的传感器结点故障或失效；

(2) 环境条件变化可能造成无线通信链路带宽变化，甚至时断时通；

(3) 传感器网络的传感器、感知对象和观察者这三要素都可能具有移动性；

(4) 新结点的加入。

由于以上因素的影响，要求无线传感器网络系统要能够适应这些因素的变化，具有动态的系统可重构性。

4. 可靠性

无线传感器网络特别适合部署在恶劣环境或人类不宜到达的区域，结点可能工作在露天环境中，遭受日晒、风吹、雨淋，甚至遭到人或动物的破坏。传感器结点往往采用随机部署，如通过飞机撒播或发射炮弹到指定区域进行部署。在这些特殊的应用场合中，都要求传感器结点非常坚固，不易损坏，以适应各种恶劣环境条件。

由于监测区域环境的限制以及传感器结点的数量巨大，不可能人工"照顾"每个传感器结点，网络的维护十分困难甚至不可维护。无线传感器网络的通信保密性和安全性也十分重要，要防止监测数据被盗取和伪造。因此，传感器网络的软硬件必须具有鲁棒性和容错性。

5. 以数据为中心

众所周知，互联网是先有计算机终端系统，然后再互联成为网络，终端系统可以脱离网络独立存在。在互联网中，网络设备用网络中唯一的 IP 地址标识，资源定位和信息传输依赖于终端、路由器、服务器等网络设备的 IP 地址。如果想访问互联网中的资源，首先要知道存放资源的服务器 IP 地址。可以说现有的互联网是一个以地址为中心的网络。

而传感器网络是任务型的网络，脱离传感器网络谈论传感器结点没有任何意义。传感器网络中的结点采用结点编号标识，结点编号是否需要全网唯一取决于网络通信协议的设计。由于传感器结点随机部署，构成的传感器网络与结点编号之间的关系是完全动态的，表现为结点编号与结点位置没有必然联系。用户使用传感器网络查询事件时，直接将所关心的事件通告给网络，而不是通告给某个确定编号的结点。网络在获得指定事件的信息后汇报给用户。这种以数据本身作为查询或传输线索的思想更接近于自然语言交流的习惯。所以通常说传感器网络是一个以数据为中心的网络。

例如，在应用于目标跟踪的传感器网络中，跟踪目标可能出现在任何地方，对目标感兴趣的用户只关心目标出现的位置和时间，并不关心哪个结点监测到目标。事实上，在目标移动的过程中，必然是由不同的结点提供目标的位置消息。

6. 集成化

传感器结点的功耗低，体积小，价格便宜，实现了集成化。其中，微机电系统技术的快速发展为无线传感器网络结点实现上述功能提供了相应的技术条件。在将来，类似"灰尘"大小的微型传感器结点也将会被研发出来。

7. 密集的结点布置

在安置传感器结点的监测区域内，布置有数量庞大的传感器结点。通过这种布置方式可以对空间抽样信息或者多维信息进行捕获，通过相应的分布式处理，即可实现高精度的目标检测和识别。同时，也可以降低单个传感器的精度要求。密集布置结点之后，将会存在大多的冗余结点，这一特性能够提高系统的容错性能，使系统对单个传感器的要求大大降低。此外，适当将其中的某些结点进行休眠调整，还可以延长网络的使用寿命。

8. 以协作方式执行任务

这种方式通常包括协作式采集、处理、存储以及传输信息。通过协作的方式，传感器的结点可以共同实现对对象的感知，得到完整的信息。这种方式可以有效克服处理和存储能力不足的缺点，共同完成复杂的任务。在协作方式下，传感器结点之间的远距离通信，可以通过多跳中继转发，也可以通过多结点协作发射的方式进行。

9. 结点唤醒方式

无线传感器网络中，结点的唤醒方式有以下几种：

1）全唤醒模式

这种模式下，无线传感器网络中的所有结点同时唤醒，探测并跟踪网络中出现的目标，虽然这种模式下可以得到较高的跟踪精度，然而是以传感器能量的巨大消耗为代价的。

2）随机唤醒模式

这种模式下，无线传感器网络中的结点由给定的唤醒概率 P 随机唤醒。

3）由预测机制选择唤醒模式

这种模式下，无线传感器网络中的结点根据跟踪任务的需要，选择性地唤醒对跟踪精度收益较大的结点，通过当前的信息预测目标下一时刻的状态，并唤醒结点。由预测机制选择唤醒模式可以获得较低的能耗损耗和较高的信息收益。

4）任务循环唤醒模式

这种模式下，无线传感器网络中的结点间歇地工作在唤醒状态，在这种工作模式下的结点可以与其他工作模式的结点共存，并协助其他工作模式的结点工作。

4.2.5 无线传感器网络安全体系

由于无线传感器的资源有限，网络往往运行在十分恶劣的环境中，因此很容易受到恶意

攻击。无线传感器网络面临的安全威胁与传统移动网络相似。

1. 无线传感器网络面临的安全威胁

无线传感器网络面临的安全威胁主要包括干扰、截取、篡改、假冒等类型。

1）干扰

干扰是指使正常的通信信息丢失或不可用。传感器大多采用无线通信方式，只要在通信范围之内，攻击者便有可能使用干扰设备发射无线电干扰信号对正常的通信信号进行干扰。也有可能在传感器结点中注入恶意代码或指令，使整个无线传感器网络瘫痪。

2）截取

截取就是攻击者使用专用的设备获取传感器结点或基站、网关、后台数据库中的重要信息。

3）篡改

篡改就是攻击者并没有获得操作传感器结点的能力，但是却对传感器通信的正常数据进行修改，或者使用非法设备发送大量假的数据包到通信系统中，把正常数据淹没在假数据的海洋中，使本来数据处理能力就不高的传感器结点无法正常工作。

4）假冒

假冒就是使用非法设备冒充正常设备，潜入到传感器网络中，参与正常通信，获取信息。或者使用假冒的数据包参与网络通信，使正常通信延迟，或者诱导正常数据，获取敏感信息。

2. 无线传感器网络的信息安全需求

无线传感器网络的信息安全需求的总目标是要保证网络中传输信息的安全性。无线传感器网络的信息安全需求主要包括以下七个方面。

1）机密性

机密性是指传输的信息对非授方是保密的，机密性是确保无线传感器网络结点间传输的敏感信息（例如传感器身份、密钥等）安全的基本要求。如上所述，无线通信的广播特性使得信息很容易截取，机密性可以使攻击方即使在截获结点间的通信信号的情况下也无法掌握这些信息的真实内容。

2）完整性

无线传感器网络的工作环境给恶意攻击者实施数据篡改或破坏提供了方便。完整性要求网络结点收到的数据包在传输过程中未执行插入、删除、篡改等操作，即保证收到的信息与发送方发出的信息是完全一致的。

3）真实性

无线传感器网络的真实性需求主要体现在点到点的信息认证和广播认证上。点到点的信息认证是指任何一个结点在收到来自另一个结点的信息时，能够核实这一信息来源的真实性，即不能被假冒或伪造。广播认证则能够核实单一结点向一组结点发送信息时的真实性。

4）可用性

可用性要求无线传感器网络能够随时按预先设定的工作方式向系统合法用户提供信息访问服务，但攻击者往往通过复制、伪造和信号干扰等方式使无线传感器网络处于全部瘫痪或部分瘫痪的状态，从而破坏系统的可用性。此外，无线传感器网络为保证安全而增加的计

算和通信量将消耗额外的能量，也会削弱无线传感器网络的可用性。

5）新鲜性

无线传感器网络由多个传感器结点组成，其多路径消息传输机制可能使接收方收到延迟的相同的数据包。新鲜性要求接收方收到的数据包始终都是最新的、非重放攻击的，即体现消息的时效性。无线传感器网络中共享密钥的传输对新鲜性比较敏感，易受重放攻击。

6）鲁棒性

无线传感器网络通信具有很强的动态性和不确定性，例如网络拓扑结构的变化、结点的加入或删除、面临攻击的多样性等。无线传感器网络对各种安全威胁应具有较强的适应性和存活性，即使某个攻击行为得逞，因为鲁棒性要求它的影响被最小化，所以单个结点受到威胁不会导致整个网络瘫痪。

7）访问控制

访问控制要求能够对访问无线传感器网络的用户身份进行确认，确保其合法性。但是传感器网络不同于传统的互联网，它并没有进、出网络的概念，每一个结点都是可以访问的，不能使用防火墙等技术来进行访问控制；无线传感器网络资源受限的特性也使得传统的基于非对称密码机制的数字签名和公钥证书机制难以应用。因此，必须建立一套适合无线传感器网络特点的，综合考虑安全性、效率和性能的访问控制机制。

3. 无线传感器网络安全体系

如上所述，无线传感器网络由多个传感器结点、网关结点、基站和后台应用系统等组成。通信链路位于传感器与传感器之间、传感器与网关结点之间和网关结点与后台系统之间。对于攻击者来说，这些设备和通信链路都有可能成为攻击的目标。

为了实现无线传感器网络的安全需求，必须综合运用多种不同的安全技术。设计并实现无线传感器网的安全体系，是实现无线传感器网络安全的关键。无线传感器网络安全体系能够从整体上应对无线传感器网络面临的各种安全威胁，达到满意的效果。无线传感器网络安全体系通过整体安全设计和分层安全设计将无线传感器网的各类安全问题统一解决，包括认证、密钥管理、安全路由等，无线传感器网络安全体系的结构如图 4-10 所示。

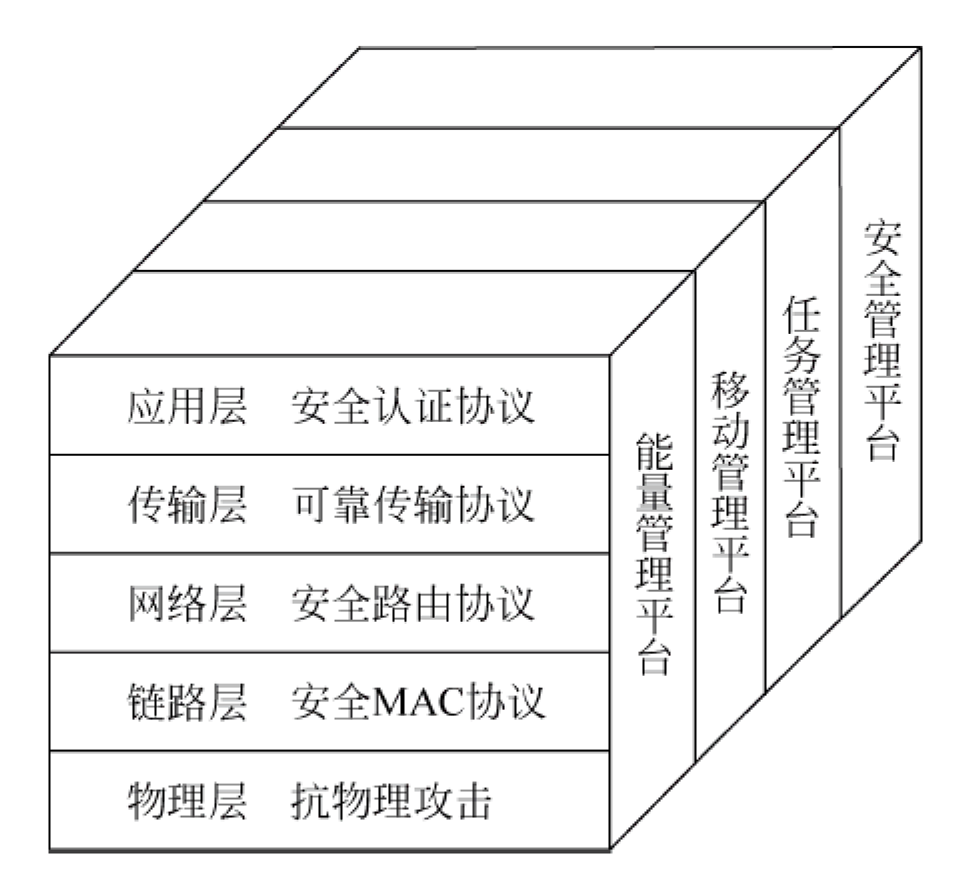


图 4-10 无线传感器网络的安全体系结构

对于无线传感器网络来说，提供安全机制和协议对系统进行安全防护是十分必要的。物理层需要对抗结点被捕获，通信链路层需要满足机密性、完整性和真实性。但是，仅仅保护传感器网络中两个结点间的通信信道的安全是不足够的。网络的核心协议，即提供服务的协议集也应该是安全的。网络协议和服务必须足以对抗任何可能的恶意攻击，以抵御来自无线传感器网络内外的安全威胁。

4.2.6 无线传感器网络物理层安全技术

在无线传感器网络中，物理层主要包括传感器的结点电路和天线两部分。对于结点电路部分，要求在实现传感器结点基本功能的基础上，分析其电路组成，测试其功耗及各个元器件的功耗，综合各种设计方案的优点，设计出廉价、低功耗、性能稳定、多传感器的结点电路方案。对于天线部分，则要求分析各种传感器结点的天线架构，测试它们的性能并进行分析，设计出低功耗、抗干扰、通信质量好的天线。

为了保证结点的物理层安全，必须解决结点的身份认证和通信问题。应研究使用合适的天线来解决结点间的通信，保证各个结点间及基站与结点间可以有效地互相通信。研究多信道问题，防范针对传感器结点的物理攻击。

1. 安全无线传感器结点

安全无线传感器结点由数据采集单元、数据处理单元及数据传输单元三部分组成，其结构如图 4-11 所示。

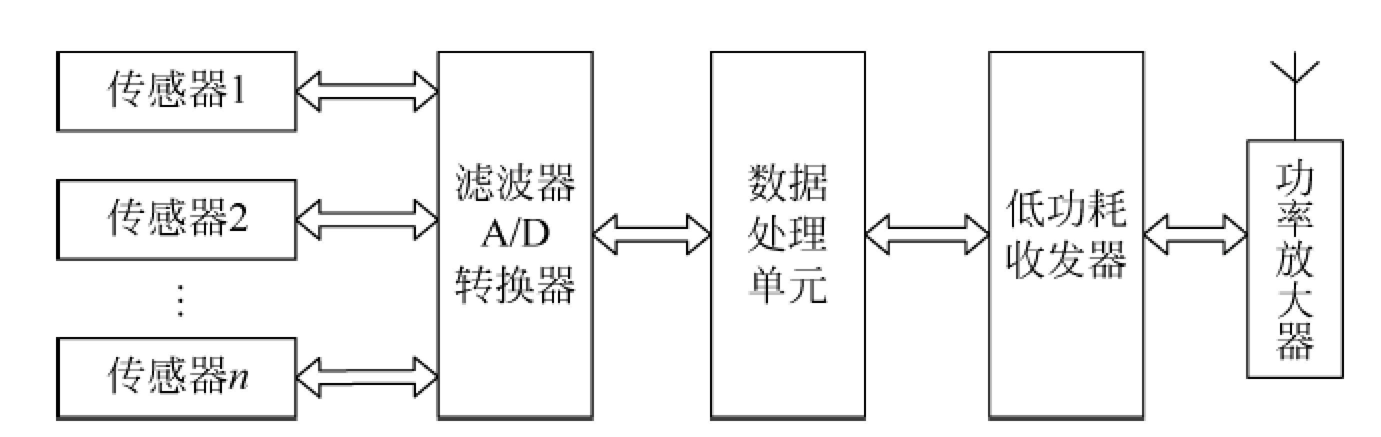


图 4-11 安全无线传感器结点的结构

无线传感器网络工作时，每个结点首先通过数据采集单元，将周围环境的特定信号转换成电信号，然后将得到的电信号传输到滤波电路和 A/D 转换电路，送入数据处理单元进行处理，最后由低功耗收发器将从数据处理单元中得到的有用信息以无线通信的方式传输出去。

安全无线传感器网络结点具有体积小、空间分布广、结点数量多、动态性强等特点，通常采用电池对结点提供能量。然而电池的能量有限，一旦某个结点的电能耗尽，该结点将退出整个网络。如果有大量的结点退出网络，网络将失去作用。因此，在电路设计中，低功耗设计是一项重要的任务。在硬件方面，可以采用太阳能电池来补充能源，并使用低功耗的微处理器和射频芯片；在软件方面，则可以关闭数据采集单元和数据传输单元，并将数据处理单元转入休眠状态。

2. 天线设计

由于无线传感器网络的设备要求体积小、功耗低，因此在设计这类无线通信系统时一般

都采用微带天线。微带天线具有体积小、质量轻、电性能多样化、易集成、能与有源电路集成为统一的组件等众多优点。但是，受到其结构和体积限制，微带天线存在频带窄、损耗较大、增益较低、仅向一半空间辐射、功率容量较低等缺点。

IEEE 802.15.4 标准是针对低速无线个域网制定的一个标准。这个标准采用倒 F 天线，工作频段为 2.4 GHz 或 868/915 MHz 频段，为个人或家庭范围内的不同设备之间的无线通信提供统一的平台，可以实现低能量消耗、低速率传输、低成本的目标。

3. 物理层攻击的防护

物理层攻击可能通过手动微探针探测、激光切割、聚集离子束操纵、短时脉冲波形干扰、能量分析等方法实施，相应的安全防护手段包括：

(1) 在任何可观察的反应和关键操作间加入随机时间延迟；

(2) 设计多线程处理器，在两个以上的执行线程间随机地执行指令；

(3) 建立传感器自测试功能使得任何拆卸传感器的企图都将导致整个器件功能的损坏；

(4) 测试电路的结构破坏或失效；

(5) 在传感器的实际电路上设置金属屏蔽网。

为加强物理层的保护，可以在传感器结点加入配置防篡改模块(Tamper Proof Module，TPM)，该模块允许安全地存储证书，当传感器结点受到威胁时阻止攻击者检索证书，一旦发现针对传感器的篡改行为，配置防篡改模块就会实施自销毁，破坏存储在模块中的所有数据和密钥。在拥有足够冗余信息的传感器网络中，这是一种切实可行的解决方案。因为一个传感器结点的价值远低于被俘获所带来的损失。关键在于发现物理攻击，一个简单的方法是定期进行邻居核查。

针对外部存储器的读取攻击，一种可行的应对措施是对外部存储器进行定期检查，对断开微控制器和外部存储器的时间进行严格的限制。

4.2.7　无线传感器网络数据链路层安全技术

媒体访问控制(Media Access Control，MAC)协议处于无线传感器网络的底层，对无线传感器网络的性能有较大的影响，是保证无线传感器网络高效通信的关键网络协议之一。无线传感器网络的 MAC 协议是由传统的载波侦听多路访问(Carrier Sense Multiple Access，CSMA)协议改进而来，典型的协议有 S-MAC、SMACS/EAR、T-MAC、DMAC 等。以下着重地对 S-MAC 协议进行分析。

S-MAC 协议是在 IEEE 802.11 协议的 SC9636-006 基础上，专门针对无线传感器网络节能的特殊需求而设计的。S-MAC 协议同时采取了多种节能技术，如空闲侦听、冲突、串音和控制开销等。

无线传感器网络由多个结点组成，利用短距离多跳通信来节省能量，大部分通信都发生在对等结点之间。网内处理对网络生存期很重要，数据将作为整个消息以存储转发的方式进行处理。无线传感器网络的应用具有很长的空闲时间，并且能容忍网络传递的延迟。

1. 周期性侦听和休眠

如上所述，在多数无线传感器网络应用中，如果没有感测到事件发生，结点将长期空闲。我们假设这样一个事实，在该段时期内数据速率非常低，因此没有必要使结点一直保持侦听。S-MAC 协议通过让结点处于周期休眠状态来降低侦听时间，每个结点休眠一段时间，然后唤醒并侦听是否有其他结点想与它通信。在休眠期间，结点关闭无线装置，并设置定时器，随后来唤醒自己。

侦听和休眠的一个完整周期被称为一帧。侦听间隔通常是固定的，根据物理层和 MAC 层的参数来决定，比如无线带宽和竞争窗口大小。占空比指侦听间隔与整个帧长度之比。休眠间隔可能根据不同的应用需求而改变，它实际上改变占空比。简单而言，这些值对所有的结点都是一样的，所有结点都可以自由选择它们各自的侦听/休眠时间表。然而，为了降低控制开销，我们更希望邻居结点保持同步，也就是说它们同时侦听和同时进入休眠。值得注意的是，在多跳网络中不是所有的邻居结点都能够保持同步。如果结点 A 和结点 B 必须分别与不同的结点 C 和结点 D 同步，那么结点 A 和结点 B 可能具有不同的时间表。

结点通过周期地向它们的直接邻居广播 SYNC 包来交换它们的时间表。一个结点在预定侦听时间与它的邻居结点通信，以确保所有邻居结点能够通信，即使它们具有不同的时间表。如果结点 A 想与结点 B 通信，结点 A 必须等待直到结点 B 侦听到结点 C 发送的一个 SYNC 同步包。S-MAC 协议的一个特征是它将结点形成一个平面型的对等拓扑结构，不像簇协议，S-MAC 协议不需要通过簇头协作。相反，结点在公用时间表形成虚拟簇，与对等结点之间直接通信。该方法的一个优点是在拓扑发生变化时，它比基于簇方法健壮。该机制的不足是由于周期休眠增加了延迟，而且，延迟有可能在每跳积聚。

2. 冲突避免

如果多个邻居结点同时想与一个结点通信，它们将试图在该结点开始侦听时发送消息，在这种情况下，它们需要竞争媒体。在竞争协议中，IEEE 802.11 在冲突避免这方面做得很好。S-MAC 协议遵循类似的流程，包括虚拟载波侦听和物理载波侦听，解决隐藏终端问题的 RTS/CTS(请求发送/清除发送)交换。每个传输包中都有一个持续时间域来标识该包要传输多长时间，如果一个结点收到一个传输给另外一个结点的包，该结点就能从持续时间域知道在多长时间内不能发送数据。结点以变量形式记录该值，被称为网络分配矢量(NAV)，NAV 可以被看成一个计时器，每次计时器开始计时，结点递减它的 NAV，直到减少到 0。在传输之前，结点首先检查它的 NAV，如果它的值不为 0，结点就认为媒体忙，这被称为虚拟载波侦听。物理载波侦听在物理层执行，通过侦听信道进行可能的传输。载波侦听时间是竞争窗口内的一个随机值，以避免冲突现象。如果虚拟载波侦听和物理载波侦听都标识媒体空闲，那么媒体就是空闲的。

在开始传输前，所有发送者都执行载波侦听。如果一个结点没有获得媒体，它将进入休眠，当接收机空闲和再一次侦听时唤醒。广播分组的发送不需要 RTS/CTS，单播分组在发送者和接收者之间遵循 RTS/CTS/DATA/ACK 序列。RTS 和 CTS 成功交换后，两个结点将利用它们的休眠时间进行数据分组传输，直到它们完成传输后才遵循它们的休眠时间

表。在每个侦听间隔内,由于占空比操作和竞争机制,S-MAC 有效地标识由于侦听和碰撞产生的能量消耗。

3. S-MAC 协议实现的关键技术

1) 数据包的嵌套结构

在 S-MAC 协议中,上一层数据包包含了下一层数据包的内容。数据包传送到哪一层,那一层只需要处理属于它的部分。

2) 堆栈结构和功能

在 S-MAC 协议堆栈内,当 MAC 层接收到上层传送过来的数据包后,它就开始载波侦听。如果结果显示 MAC 层空闲,它就会把数据传到物理层;如果 MAC 层忙,它将会进入睡眠状态,直到下一个可用时间的到来,再重新发送。当 MAC 层在收到物理层传送过来的数据包后,则先通过循环冗余校验(CRC),检验是否有错误。如果没有错误,MAC 层就会将数据包传向上层。

3) 选择和维护调度表

在开始周期性侦听和睡眠之前,每个结点都需要选择睡眠调度机制并与邻居结点一致。如何选择和保持睡眠调度机制分为以下 3 种情况。

(1) 结点在侦听时间内,如果它没有侦听到其他结点的睡眠调度机制,则立即选择一个睡眠调度机制。

(2) 当结点在选择和宣布自己的调度机制之前,收到了邻居结点广播的睡眠调度机制,它将采用邻居结点的睡眠调度机制。

(3) 当结点在选择和广播自己的睡眠调度机制之后,收到几种不同的睡眠调度机制时,就要分以下两种情况考虑:当结点没有邻居结点时,它会舍弃自己当前的睡眠调度机制,采用刚接收到的睡眠调度机制;当结点有一个或更多邻居结点时,它将同时采用不同的调度机制。

4) 时间同步

在 S-MAC 协议中,结点与邻居结点需要保持时间同步来同时侦听和睡眠。S-MAC 协议采用的是相对而不是绝对的时间戳,同时使侦听时间远大于时钟误差和漂移,来减少同步误差,并且结点会根据收到的邻居结点的数据包来更新自己的时钟,从而与邻居结点保持时间同步。

5) 带冲突避免的载波侦听多路访问

带冲突避免的载波侦听多路访问(CSMA/CA)的基本机制是在接收者和发送者之间建立一个握手机制来传输数据。

握手机制是由发送端发送一个请求发送(RTS)包给它的接收者,接收者在收到以后就回复一个准备接收(CTS)包,发送端在收到 CTS 包后,开始发送数据包,RTS 与 CTS 之间的握手是为了使发送端和接收端的邻居结点知道它们正在进行数据传输,从而减少传输碰撞。

6) 网络分配矢量

在 S-MAC 协议中,每个结点都保持了一个网络分配矢量(NAV)来表示邻居结点的活动时间,S-MAC 协议中在每个数据包中都包含了一个持续时间指示值,持续时间指示值表

示目前这个通信需要持续的时间。邻居结点收到发送者或接收者发往其他结点的数据包时，就可以知道它需要睡眠多久，即用数据包中的持续时间更新 NAV 的值，当 NAV 的值不为 0 时，结点应该进入睡眠状态来避免串音。当 NAV 变为 0 时，它就马上醒来，准备进行通信。

与 IEEE 802.11 MAC 相比，S-MAC 协议尽量延长其他结点的休眠时间，从而降低了碰撞概率，减少了空闲侦听所消耗的能源；通过流量自适应的侦听机制，减少消息在网络中的传输延迟；采用带内信令来减少重传和避免监听不必要的数据；通过消息分割和突发传递机制来和带内数据处理来减少控制消息的开销和消息的传递延迟。因此 S-MAC 协议具有很好的节能特性，这对无线传感器网络的需求和特点来说是合理的。但是，因为 S-MAC 中占空比固定不变，所以它不能很好地适应网络流量的变化，而且协议的实现非常复杂，需要占用大量的存储空间。这个问题对于资源受限的传感器结点尤为突出。

4.2.8 无线传感器网络网络层安全技术

传感器网络的安全问题是一个开放的、活跃的研究领域。SPINS 安全体系是目前研究者提出的传感器网络安全体制中比较流行、实用的无线传感器网络安全方案。它在数据机密性、完整性、新鲜性、可认证等方面都做了充分的考虑。

SPINS 安全协议包含 SNEP(Security Network Encryption Protocol)和 μTESLA(micro Timed Efficient Streaming Loss-tolerant Authentication)两个部分。SNEP 用以实现通信的机密性、完整性、新鲜性和点到点的认证；μTESLA 用以实现在资源受限的情况下的点到多点的广播认证。

1. 安全网络加密协议 SNEP

SNEP 协议是一个低通信开销的，实现了数据机密性、数据认证、完整性保护、新鲜性保证的简单高效的安全通信协议，为传感器网络量身打造本身只描述安全实施的协议过程，并不规定实际使用的算法，具体的算法在具体实现的时候考虑。

SNEP 协议采用预共享主密钥的安全引导模型，假设每个结点都和基站之间共享一对主密钥，其他密钥都是从主密钥衍生出来的。SNEP 协议的各种安全机制都是通过信任基站完成的。

1) SNEP 协议的机密性

SNEP 协议实现的机密性不仅仅具有加密功能，还具有语义安全特性，语义安全特性是针对数据机密性提出的一个概念，它的含义是指相同的数据信息在不同的时间、不同的上下文，经过相同的密钥和加密算法产生的密文不同。语义安全性可以有效抑制对明文的攻击。实现语义安全性的方法很多，使用密码分组链(Cipher Block Chaining，CBC)加密模式具有先天的语义安全特性，因为每块数据的密文是将自身与前段密文迭代异或产生的；计数器(CounTeR，CTR)模式也可以实现语义安全，因为每个数据包的密文与其加密时的计数器值相关。在 CTR 模式中，通信双方共享一个计数器，计数器值作为每次通信加密的初始化向量(Initial Vector，IV)。这样，每次通信时的计数器值不同，相同的明文必定产生不同的密文。SNEP 协议采取计数器模式的加密方法实现语义安全机制，其加密公式如下所示：

$$E = \{D\}(K_{enc}, C)$$

其中,E 表示加密后的密文,D 表示加密前的明文,K_{enc}表示加密密钥,C 表示计数器,用作块加密的初始向量。

2) SNEP 协议的完整性和点到点认证

SNEP 协议实现消息完整性和点到点认证是通过消息认证码(Message Authentication Code,MAC)协议实现的。消息认证码协议的认证公式定义如下:

$$M = \text{MAC}(K_{mac}, C \mid E)$$

其中,K_{mac}表示消息认证算法的密钥,$C|E$ 为计数器值和密文的粘接,表明消息认证码是对计数器和密文一起进行运算。消息认证的内容可以是明文,也可以是密文,SNEP 采用的是密文认证。用密文认证方式可以加快接收结点认证数据包的速度,接收结点在收到数据包后可以马上对密文进行认证,发现问题直接丢弃,无须对数据包进行解密。明文认证过程则是接收结点必须先解密再认证,会推迟错误的数据包的辨认时机,浪费结点计算资源,同时使系统对攻击更加敏感。另外,逐跳认证方式只能选择密文认证的方式,因为中间没有端到端的通信密钥,不能对加密的数据包进行解密。

K_{enc}和 K_{mac}这两个密钥都是通过与基站共享的主密钥 K_{master}按照相同的算法推演出来的。SNEP 没有定义推演算法,实现者可以按照一定的规则来生成加密密钥 K_{enc}和认证密钥 K_{mac}。

在加州大学伯克利分校提出的 SNEP 模型系统中,直接使用 μTESLA 协议中定义的单向散列函数 F 来生成加密密钥 K_{enc}和认证密钥 K_{mac}:

$$K_{enc} = F^{(1)}(K_{master})$$

$$K_{mac} = F^{(2)}(K_{master})$$

一个完整的结点 A 到结点 B 之间的交换过程如下所示:

$$A \rightarrow B: \{D\}(K_{enc}, C), \text{MAC}(K_{mac}, C \mid \{D\}(K_{enc}, C))$$

3) SNEP 协议的新鲜性认证

SNEP 协议通过 CTR 模式支持数据通信的弱新鲜性。所谓弱新鲜性是指一种单向的新鲜性认证。假如结点 A 给结点 B 连续发送 10 个请求数据包,通过计数器值能够知道这 10 个请求数据包是顺序从结点 A 发送出来的。得到这 10 个请求包以后,结点 B 会将请求交给其上层应用层处理,并将相应消息回复给结点 A,结点 A 从结点 B 收到 10 个回复消息。结点 A 同样根据计数器值可以判断这 10 个响应包是从结点 B 顺序发送出来的,并且对于任何响应包的重放攻击都能有效抑制,即实现了弱新鲜性认证。

这种新鲜性认证存在一个问题,结点 A 不能判断它所收到的响应包是针对它发出的哪个请求包的回应。如果 A 收到的回复消息不是按照其请求包发送顺序给出的,那么它将不能为每个请求回送正确的响应。为此,SNEP 协议定义了强新鲜认证方法。

SNEP 协议使用 Nonce 机制实现强新鲜特性。Nonce 是一个唯一标识当前状态的、任何无关者都不能预测的随机数,它通常由真随机数发生器产生。SNEP 协议在其强新鲜认证过程中,在每个安全通信的请求数据包中增加 Nonce 段,用来唯一标示请求包的身份。为了保证安全性,Nonce 要足够长,以避免被攻击者预测出来,减少碰巧相同的概率。

结点 A 在发送给结点 B 的消息中增加一个 Nonce 段:N_A,结点 B 在对该消息应答的时候让 N_A 参加回应包的消息认证计算,并返回给结点 A。这样,结点 A 就可以通过响应包

的认证码得知这个回应是针对 N_A 标示的请求消息给出的，不必考虑回应的顺序问题。

4）用 SNEP 协议完成结点间的通信

使用 SNEP 协议完成结点间通信的一种可行方法是通过信任基站为将要通信的两个结点建立临时通信密钥。假设结点 A 和结点 B 都与基站 S 存在共享密钥 K_{AS} 和 K_{BS}，则安全信道的建立过程如下：

A→B：N_A，A

B→S：N_A，N_B，A，B，MAC(K_{BS}，$N_A|N_B|A|B$)

S→A：N_A，{ SK_{AB} } K_{AS}，MAC(K_{AS}，$N_A|B|$ { SK_{AB} } K_{AS})

S→B：N_A，{ SK_{AB} } K_{BS}，MAC(K_{BS}，$N_B|A|$ { SK_{AB} } K_{BS})

SK_{AB}是基站 S 为结点 A 和 B 设定的临时通信密钥，N_A 和 N_B 是强新鲜认证的 Nonce 随机数，在结点之间的通信完成后，双方可以直接丢弃这个信任密钥。如果以后再需要通信，可以重新生成临时通信密钥。

2．基于时间的高效的容忍丢包的流认证协议μTESLA

为了节省网络带宽和通信时间，基站经常采取广播的方式向结点发送消息。结点接收广播包的时候，必须要能够对广播包的来源进行认证，否则结点很容易受到 DoS 广播攻击。广播包的认证和单播包的认证过程不同，单播包的认证只要收发结点之间共享一对认证密钥就可以完成了，而广播包则要使用一个全网的公共密钥来完成认证。广播包认证是一个单向的认证过程，所以必须使用非对称密钥机制来完成。通过 SNEP 协议实现广播包的认证，只能通过复制数据包，以单播包的形式传播到所有结点，这样的开销非常巨大。

最直接的解决办法是基站和所有结点共享一个公共的广播认证密钥，结点使用这个密钥进行广播包的认证。但这种方法安全度很低，因为任何一个结点被俘都会泄露整个网络的广播密钥。使用一包一密钥的认证方式，可以防止被俘结点泄露秘密，但是需要不断更新密钥，增加通信开销，且更新密钥的过程又是一个需要认证的广播过程。

Adrian Perrig 等人提出了微型基于时间的高效的容忍丢包的流认证协议 μTESLA (micro Timed Efficient Streaming Loss-tolerant Authentication)。该协议以 TESLA 协议为基础，对密钥更新过程、初始化认证过程进行了改进，使之能够在无线传感器网中有效实施。

1）μTESLA 协议基本思想

认证广播协议的安全条件是“没有攻击者可以伪造正确的广播数据包”。μTESLA 协议就是依据这个安全条件来设计的。认证本身不能防止恶意结点制造错误的数据包来干扰系统的运行，只保证正确的数据包一定是由授权的结点发送出来的。μTESLA 协议的主要思想是先广播一个通过密钥 K_{mac} 认证的数据包，然后公布密钥 K_{mac}，这样就保证了在密钥 K_{mac}公布之前，没有人能够得到认证密钥的任何信息，也就没有办法在广播包正确认证之前伪造出正确的广播数据包。这样的协议构成恰好满足流认证广播的安全条件。

μTESLA 协议在设计过程中解决的问题如下：

（1）共享密钥问题。

结点必须能够首先认证公布的密钥，进而用密钥认证数据包。μTESLA 协议采用的是全网共享密钥生成算法的方法，而不是共享密钥池。真正的密钥池只在广播者（基站）中存

放。这样,无论实际的密钥池有多大,对结点来说都只需要存放相同的一段代码。

(2) 密钥生成算法的单向性问题。

因为全网共享的秘密是密钥生成算法,若正常结点被俘获,将暴露这个密钥生成算法。密钥发布包是明文广播,所以恶意结点和正常结点一样可以获得密钥明文。μTESLA 协议为了防止恶意结点根据已知密钥明文和密钥生成算法推测出新的认证密钥,使用单向散列函数来解决密钥生成问题。单向散列函数的特性就是其逆函数不存在或者计算复杂度非常大。这样即使恶意结点拥有了算法和已经公开的密钥,仍然不能推算出下一个要公布的密钥是什么。

(3) 密钥发布包丢失问题。

无线信道是一个没有质量保证的信道,数据冲突和丢失的可能性很大。如果一个结点丢失了密钥发布包,就会导致一个时段收到的广播数据包不能被正确认证。μTESLA 协议之所以称为容忍丢失的流认证协议,最重要的一点就是它引入了密钥链机制,解决了密钥发布包丢失给认证带来的问题。该机制要求基站密钥池中存放的密钥不是相互独立的,而是经过单向密钥生成算法由迭代运算产生出来的一串密钥。已知祖先密钥,可以用单向散列函数产生所有的子孙密钥。这样即使中间丢失几个发布的密钥,仍然可以根据最新的密钥把它们推算出来。

(4) 时间同步和密钥公布延迟问题。

为了解决拥塞问题和延迟问题,μTESLA 协议使用了周期性公布认证密钥的方式,一段时间内使用相同的认证密钥。这样的处理对于广播包频率较高的应用特别高效,对于频率低的应用也不会增加认证延迟。周期性更新密钥要求基站和结点之间要维持一个简单的同步,这样结点就可以通过当时时钟判断公布的密钥是哪个时间段使用的密钥,然后用该密钥对该时间段中接收到的数据包进行认证。密钥使用时间和密钥公布时间的延迟是需要权衡的,太长可能导致结点需要大的存储空间来缓存收到的广播包,太短会频繁切换密钥导致通信消耗过大。延迟时间的定义可以根据广播包的发送频率确定。

(5) 密钥认证和初始化问题。

结点对于每个收到的密钥,首先要确认它是从信任基站发送出来的,而不是一个恶意结点伪造的。密钥生成算法的单向特性为密钥的确认提供了很好的手段。因为密钥是单向可推导的,所以根据前面获得的合法密钥可以验证新收到的密钥是不是合法的密钥。结点用单向密钥生成算法对新收到的密钥进行运算,如果能够得到原来收到的合法密钥,并且满足时间同步要求,那么新收到的密钥是合法的,否则是不合法的。但这个过程要求初始第一个密钥必须是确认合法的。这个初始认证是通过协议初始化过程完成的。μTESLA 协议使用 SNEP 协议来进行初始认证密钥和同步时间的协商。

2) μTESLA 协议的实现过程

μTESLA 协议通过对称密钥的延迟透露而引入非对称性来产生有效的广播认证,μTESLA 协议通常由 4 个阶段组成,即密钥建立、广播密钥透露、感知结点自举、认证广播数据包。

(1) 密钥建立。

发送者首先生成一个密钥序列(密钥链),为了产生一个长度为 n 的单向密钥链,基站随机选择一个密钥 K_n,并且通过使用一个单向散列函数 F,相继产生其他的密钥:

$$K_i = F(K_{i+1})$$

(2) 广播密钥透露。

传感器网络的生存时间被分成 n 个时间间隔,主机把密钥链中的每个密钥和相应的时间间隔对应起来。在时间间隔 t 内,主机使用当前密钥 K_t 来计算在这个时间间隔内数据包的信息认证码。然后主机将时间间隔 t 后延迟 δ 个时间间隔广播密钥 K_t,这里,δ 为密钥透露延时,其值由信息新鲜度要求和传感器的存储能力决定。

(3) 感知结点自举。

单向密钥链的一个很重要的特性,是接收者通过使用一个认证密钥可以轻易地认证单向密钥链中的后继密钥。例如,如果接收者有一个密钥链中的认证密钥 K_i,就很容易通过计算 $K_i=F(K_{i+1})$来验证 K_{i+1}。因此,每个结点都需要密钥链上的一个可信密钥作为该链的密钥头,并且知道密钥的透露时间表。

(4) 认证广播数据包。

一旦结点接收到一个先前时间间隔的密钥 K_j,就使用如下所示的单向函数 F 来验证其是否等于前面发布的可信密钥 K_i:

$$K_i = F^{i-j}(K_j)$$

如果相等则表示新密钥 K_j 可信,接收者可以用密钥 K_j 认证在时间间隔 i 到 j 内接收的所有数据包,同时接收者用 K_j 代替 K_i 成为新的可信密钥。

结点认证广播包的过程为:在时间间隔$[T_i, T_i+T_{int}]$内,基站发送广播包 P_1 和 P_2。结点接收到广播包后通过时间同步条件判断,它们公布的广播密钥 K_i 还没有发布出来,于是把广播包保存起来,等待该密钥的发布。在 T_{i+2}时刻,基站发布 K_i,结点计算 $F(K_i)$,检验是否等于 K_{i-1},如果相同,则 K_i 就是合法密钥;否则 K_i 就不是合法密钥,应丢弃此密钥。验证通过后,结点就根据时间标尺自动使用 K_i 来认证 P_1 和 P_2。假如没有收到 K_i,结点会把 P_1 和 P_2 包的认证推迟到接收下一个密钥 K_{i+1}时。收到 K_{i+1}后结点会通过计算 $F(F(K_{i+1}))$,看其结果是否等于 K_{i-1}来确定密钥是否合法。如果合法,则用下式计算 K_i,用 K_i 对 P_1 和 P_2 进行认证。

$$K_i = F(K_{i+1})$$

整个广播数据包的认证过程如图 4-12 所示。

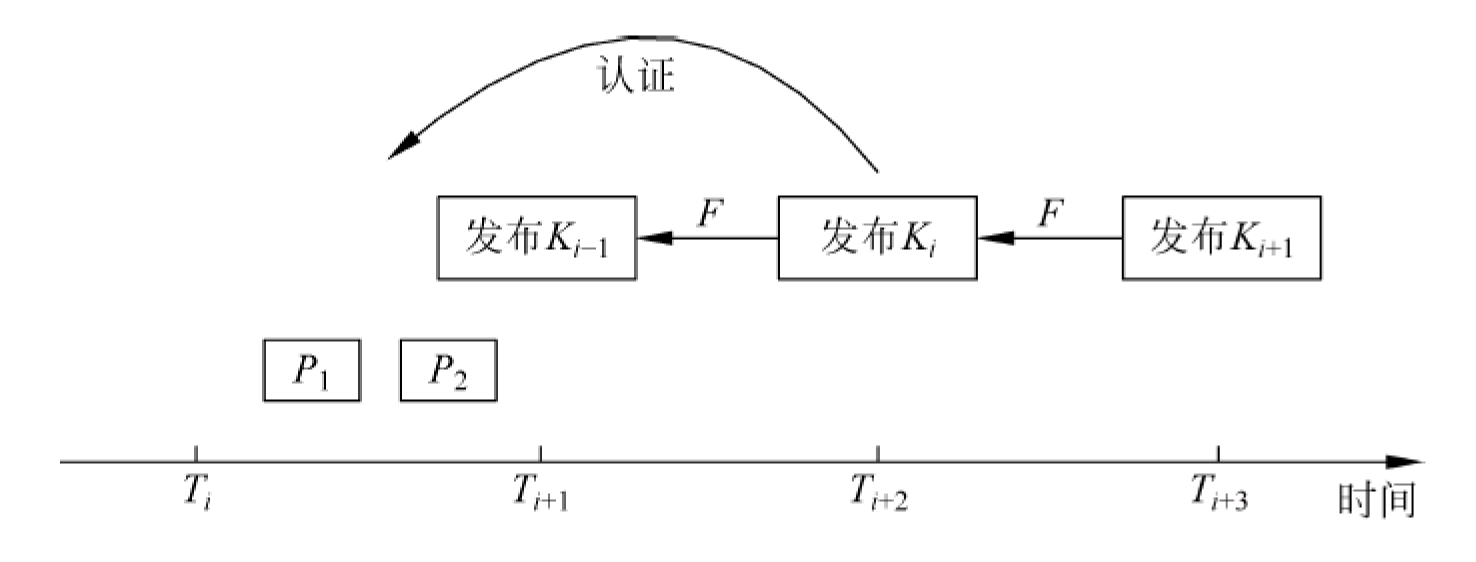


图 4-12 μTESLA 广播数据包的认证

4.2.9 无线传感器网络路由协议

无线传感器网络安全路由协议的设计是一个技术难题,无线传感器网络中所有结点都

应可达(连通性),网络结点还要求尽量多地覆盖目标区域,并且要容许无线传感器网络中部分结点由于能量或其他原因无法正常工作。安全路由算法也要能适应不同的网络规模和结点密度,并要具有一定的服务质量要求。因此,除了低存储器容量、低功耗以外,无线传感器网络的安全是设计者不可忽视的重要因素。

无线传感器网络的攻击者都希望控制路由器,以便截取、篡改、欺骗或丢弃网络中传输的数据包。攻击者可以通过广播自己控制的结点有更好的连通性或通信速度的方式来将网络中的数据流导向自己控制的结点;攻击者也可能篡改路由控制数据包。

对于任何路由协议,路由失败将导致网络的数据传输能力下降,严重的会导致整个网络瘫痪。如何在动态拓扑、有限计算能力和严格能量约束的网络环境中确保安全路由的实现是一个挑战。

目前,适用于无线传感器网络的路由协议比较多,主要分为单层路由协议、多层路由协议和基于地理位置的路由协议三大类。

典型的单层无线传感器网络路由协议包括 SPIN 协议、Directed Diffusion 协议和谣言协议等。

多层路由协议与单层路由协议相比较,具有更好的可扩展性,更易于进行数据融合,从而减少能量的消耗。在单层路由协议中,由于网络规模的扩大,网关的负载将加大,导致网络延时增大。典型的多层路由协议包括 LEACH 协议、PEGASIS 协议、TEEN 协议和 SEC-Tree 协议等。

基于地理位置的路由协议需要知道传感器结点的位置信息,这些信息可用于计算结点之间的距离、估计能量的消耗以及构建更加高效的路由协议。由于无线传感器结点散布在一个区域内,并且没有类似 IP 地址这样的地址方案,因而可以利用位置信息来构建高效的路由协议,以延长网络的寿命。典型的基于地理位置的路由协议包括 GPSR 协议、GEAR 协议和 TBF 协议等。

1. SPIN 协议

基于信息协商的传感器协议(Sensor Protocol for Information via Negotiation,SPIN)是一种以数据为中心的自适应通信路由协议。它通过使用结点间的协商制度和资源自适应机制,来解决泛洪算法中的“内爆”和“重叠”问题,节省了能量的消耗。SPIN 协议有 3 种数据包类型,即 ADV、REQ 和 DATA。ADV 用于元数据的广播,REQ 用于请求发送数据,DATA 为传感器采集的数据包。SPIN 协议以抽象的元数据为数据命名,结点收到数据后,为了避免盲目传播,用包含元数据的 ADV 消息向邻结点通告,需要数据的邻结点用 REQ 消息提出请求,数据通过 DATA 消息发送到请求结点。

传感器结点采用 SPIN 协议交互的基本过程如下:

(1) 结点 A 采集到数据 m。向外广播带有 m 元数据(元数据指数据的属性)的 adv 数据包。

(2) 邻居结点 B 收到 A 的 adv 数据包,根据其携带的元数据判断自身是否需要数据 m。如果不需要,则销毁 adv 数据包。需要则生成相应的 req 数据包,向外广播。

(3) 结点 A 收到 B 的 req 数据包请求,生成相应的 data 数据包相外广播。

(4) 结点 B 收到 A 的 data 数据包,进行数据 m 的存储。

(5) 结点 B 继续向外广播带有 m 元数据的 adv 数据包,从而数据 m 在网络中被传递。

每个结点都拥有一个唯一的地址,称为结点的自身地址。当结点 A 自身随机采集到有效数据 m 的时候,A 立即生成与数据 m 相匹配的元数据,并将元数据和自身的地址封装成 adv 数据包,将其向外广播。

当 A 的邻居结点 B 收到 adv 数据包后,它首先提取 adv 数据包的元数据域,查看其元数据是否为自身需要的数据属性,如果不需要,则销毁 adv 数据包;如果需要,则提取 adv 数据包中的 A 结点的地址作为目的地址,将其和元数据以及自身地址封装成相应的 req 数据包向外广播。

这样结点 A 又收到了 req 数据包。首先,A 要提取 req 数据包中的目的地址,判断其是否和自身的地址相同。不相同则表示此 req 不是自身需要的,则销毁 req 数据包。相同则表明此数据包是发给自身的。提取其源地址作为目的地址,提取其元数据域,找到与元数据相匹配的自身数据一同封装生成相应的 data 包向外广播。

邻居结点 B 收到 data 包之后,也同样的通过检查其目的地址来判断其是否为自身所需要的 data 包。相符则存储数据,否则销毁数据包。当数据真正的存储到了 B 结点之后,也就完成了一个数据的转移。此时,结点 B 可以发送 adv 数据包,通知其他邻居结点,结点 B 拥有这个数据,从而达到将数据传播出去的目的。

SPIN 协议的主要优点包括:通过小 ADV 消息减轻了“内爆”问题;通过数据命名解决了“重叠”问题;结点根据自身资源和应用信息决定是否进行 ADV 通告,避免了盲目利用资源的问题,有效地节约了能量。

SPIN 协议的主要缺点包括:当产生或收到数据的结点的所有邻结点都不需要该数据时,将导致数据不能继续转发,以致较远结点无法得到数据。当网络中汇聚(Sink)结点较少时,问题就变得比较严重;当某汇聚结点对所有数据都需要时,其周围结点的能量容易耗尽。SPIN 协议虽然在一定程度上减轻了数据内爆,但是在较大规模的网络中,ADV 内爆问题仍然存在。

2. Directed Diffusion 协议

定向扩散路由协议(Directed Diffusion,DD)是一种专为传感器网络设计的路由协议,这个协议是以数据为中心的路由协议的一次飞跃,此后许多路由协议都是以这个协议为基础提出的。

Directed Diffusion 协议的实现过程包括三个阶段:兴趣扩散,梯度建立以及路径加强。

1) 兴趣扩散

汇聚结点查询兴趣消息,兴趣消息采用泛洪的方法传播到网络,来通知整个网络中的其他结点它需要的信息。

2) 梯度建立

在兴趣消息扩散的同时相应的路由路径也建立完成。有“兴趣消息”相关数据的普通结点将自己采集的数据通过建立好的路径传送到汇聚结点。

3) 路径加强

最后汇聚(sink)结点选择一条最优路径作为强化路径。

Directed Diffusion 协议是一个单层路由协议,主要是解决网络中存在多个汇聚(sink)

结点及汇聚结点移动的问题。当多个结点探测到事件发生时，选择一个结点作为发送数据的源结点，源结点以自身作为格状网(grid)的一个交叉点构造一个格状网。其过程是：源结点先计算出相邻交叉点位置，利用贪心算法请求最接近该位置的结点成为新交叉点，新交叉点继续该过程直至请求过期或到达网络边缘交叉点保存了事件和源结点信息。进行数据查询时，sink 点本地 flooding 查询请求到最近的交叉结点，此后查询请求在交叉点间传播，最终源结点收到查询请求，数据反向传送到 sink 点。sink 点在等待数据时，可继续移动，并采用代理(Agent)机制保证数据可靠传递。与 Directed Diffusion 协议相比，该协议采用单路径，能够提高网络生存时间，但计算与维护格状网的开销较大；结点必须知道自身位置；非 sink 点位置不能移动；要求结点密度较大。

3. 谣言协议

谣言协议(Rumor)是在 Directed Diffusion 协议的基础上改进而来的。对于 Directed Diffusion 协议，如果 sink 结点的一次查询只须一次上报，Directed Diffusion 协议开销就太大了。Rumor 协议正是为解决此问题而设计的。

Rumor 协议借鉴了欧氏平面图上任意两条曲线交叉几率很大的思想。当结点监测到事件后将其保存，并创建称为 Agent 的生命周期较长的包括事件和源结点信息的数据包，将其按一条或多条随机路径在网络中转发。收到 Agent 的结点根据事件和源结点信息建立反向路径，并将 Agent 再次随机发送到相邻结点，并可在再次发送前在 Agent 中增加其已知的事件信息。sink 点的查询请求也沿着一条随机路径转发，当两路径交叉时则路由建立；如不交叉，sink 点可 flooding 查询请求。

在多 sink 点、查询请求数目很大、网络事件很少的情况下，Rumor 协议较为有效。但如果事件非常多，维护事件表和收发 Agent 带来的开销会很大。

4. LEACH 协议

低功耗自适应集簇分层型协议(Low Energy Adaptive Clustering Hierarchy，LEACH)是一种无线传感器网络路由协议，是第一个数据聚合的层次路由协议。基于 LEACH 协议的算法，称为 LEACH 算法。

LEACH 算法的基本思想是：以循环的方式随机选择簇头结点，将整个网络的能量负载平均分配到每个传感器结点中，从而达到降低网络能源消耗、提高网络整体生存时间的目的。与一般的平面多跳路由协议和静态分层算法相比，LEACH 分簇协议可以将网络生命周期延长 15%。

LEACH 算法在运行过程中不断地循环执行簇的重构过程，每个簇重构过程可以用回合的概念来描述。每个回合可以分成两个阶段：簇的建立阶段和传输数据的稳定阶段。为了节省资源开销，稳定阶段的持续时间要大于建立阶段的持续时间。簇的建立过程可分成 4 个阶段：簇头结点的选择、簇头结点的广播、簇头结点的建立和调度机制的生成。

簇头结点的选择依据网络中所需要的簇头结点总数和迄今为止每个结点已成为簇头结点的次数来决定。具体的选择办法是：每个传感器结点随机选择 0～1 之间的一个值。如果选定的值小于某一个阈值，那么这个结点成为簇头结点。

选定簇头结点后，通过广播告知整个网络。网络中的其他结点根据接收信息的信号强

度决定从属的簇，并通知相应的簇头结点，完成簇的建立。最后，簇头结点采用 TDMA 方式为簇中每个结点分配向其传递数据的时间点。

稳定阶段中，传感器结点将采集的数据传送到簇头结点。簇头结点对簇中所有结点所采集的数据进行信息融合后再传送给汇聚结点，这是一种较少通信业务量的合理工作模型。稳定阶段持续一段时间后，网络重新进入簇的建立阶段，进行下一回合的簇重构，不断循环，每个簇采用不同的 CDMA 代码进行通信来减少其他簇内结点的干扰。

LEACH 路由协议主要分为两个阶段：即簇建立阶段(setup phase)和稳定运行阶段(ready phase)。簇建立阶段和稳定运行阶段所持续的时间总和为一轮(round)。为减少协议开销，稳定运行阶段的持续时间要长于簇建立阶段。

在簇建立阶段，传感器结点随机生成一个 0，1 之间的随机数，并且与阈值 $T(n)$ 做比较，如果小于该阈值，则该结点就会当选为簇头。$T(n)$ 按照下列公式计算：

$$T(n)=\begin{cases}\dfrac{p}{1-p\times\left(r \bmod \dfrac{1}{p}\right)}, & n\in G\\ 0, & n\notin G\end{cases}$$

式中，p 为结点成为簇头结点的百分数，r 为当前轮数，G 为在最近的 $1/p$ 轮中未当选簇头的结点集合。簇头结点选定后，广播自己成为簇头的消息，结点根据接收到的消息的强度决定加入哪个簇，并告知相应的簇头，完成簇的建立过程。然后，簇头结点采用 TDMA 的方式，为簇内成员分配传送数据的时隙。

在稳定阶段，传感器结点将采集的数据传送到簇头结点。簇头结点对采集的数据进行数据融合后再将信息传送给汇聚结点，汇聚结点将数据传送给监控中心来进行数据的处理。稳定阶段持续一段时间后，网络重新进入簇的建立阶段，进行下一轮的簇重建，不断循环。

LEACH 协议是一种完全分布式的路由协议，结点不需要保存任何关于网络拓扑结构的信息；同时，通过动态和随机地选择簇头的方法，延长了网络的寿命。但是，在 LEACH 协议中，每一个簇头都可以直接和汇聚结点进行通信，限制了网络的规模。换言之，LEACH 协议仅适用于结点可以直接和汇聚结点进行通信的无线传感器网络。并且，动态地选择簇头需要额外的开销。

5. PEGASIS 协议

传感器信息系统能量有效聚集协议(Power Efficient Gathering in Sensor Information Systems，PEGASIS)是对 LEACH 协议的一种改进。PEGASIS 协议的基本思想是：为了延长网络的生命周期，结点只需要与它们最接近的邻居进行通信。

在 PEGASIS 协议中，结点与汇聚点间的通信过程是轮流进行的，当所有结点都与汇聚点通信后，结点间再进行新一回合的轮流进行的。由于这种轮流通信机制使得能量消耗能够统一的分布到每个结点上，因此降低了整个传输所需要消耗的能量。

不同于 LEACH 的多簇结构，PEGASIS 协议在传感器结点中采用链式结构进行链接。运行 PEGASIS 协议时每个结点首先利用信号的强度来衡量其所有邻居结点距离的远近，在确定其最近邻居的同时调整发送信号的强度以便只有这个邻居能够听到。其次，链中每个结点向邻居结点发送数据，并且只选择一个结点作为链首向汇聚结点传输数据。采集到

的数据以点对点的方式传递、融合,并最终被送到汇聚结点 PEGASIS 协议是对 LEACH 协议的改进,它减少了 LEACH 簇重构产生的能量开销,并通过数据融合技术降低了结点的能量消耗,与 LEACH 协议比较,PEGASIS 协议延长了网络生存周期大约 2 倍。

PEGASIS 协议与 LEACH 协议相比较,在节省能量方面主要体现在以下几点:

(1) 在传感器结点进行本地数据通信阶段,PEGASIS 协议的算法中,每个结点只和自己距离最近的邻居结点进行通信。在 LEACH 协议算法中,每个非簇头结点都需要直接与所在簇的簇头结点进行通信。因此,PEGASIS 协议的算法减少了每轮通信中每个结点的通信距离,从而节省了每个结点的能量。

(2) 在 PEGASIS 协议算法中,Leader 结点最多只接收两个邻居结点的数据以及向基站发送网络的数据。而 LEACH 协议的算法中,每个簇头结点除了向基站发送网络的数据之外,还要接收来自所在簇内的所有非簇头结点的数据,簇头结点接收的数据量远远大于 PEGASIS 协议中 Leader 结点所接收的数据量。所以 LEACH 协议中簇头结点的能量消耗过快,不利于均衡结点的能量消耗。

(3) 在每一轮通信的过程中,PEGASIS 协议中只有 1 个 Leader 结点与基站通信,而 LEACH 协议中有许多簇头结点与基站通信。基站的位置又是远离网络的,这样就会使得网络中结点的能量消耗过快,不利于节省能量。所以 PEGASIS 协议的网络生命周期要长与 LEACH 协议的网络生命周期。

PEGASIS 协议的主要优点是减少了 LEACH 在簇重构过程中所产生的开销,并且通过数据融合降低了收发过程的次数,从而降低了能量的消耗,与 LEACH 相比,PEGASIS 能够提高网络的生存周期近 2 倍。

PEGASIS 协议的缺点如下:

(1) PEGASIS 协议假定每个传感器结点能够直接与汇聚结点通信,而在实际网络中,传感器结点一般需要采用多跳方式到达汇聚结点;

(2) PEGASIS 协议假定所有的传感器结点都具有相同级别的能量,因此结点很可能在同一时间内全部死亡;

(3) 尽管协议避免了重构簇的开销,但由于传感器结点需要知道邻居的能量状态以便传送数据,协议仍需要动态调整拓扑结构。对那些利用率高的网络而言,拓扑的调整会带来更大的开销;

(4) 协议所构建的链接中,远距离的结点会引起过多的数据延迟,而且链首结点的唯一性使得链首会成为瓶颈。

6. TEEN 协议

阈值敏感的高效节能的传感器网络协议(Threshold-sensitive Energy Efficient sensor Network protocol,TEEN)是一种层次路由协议,利用过滤的方式来减少数据传输量。TEEN 协议采用与 LEACH 相同的多簇结构运行方式。不同的是,在簇的建立过程中,随着簇首结点的选定,簇首结点除了通过 TDMA 方法实现数据的调度,还向簇内成员广播有关数据的硬阈值和软阈值这两个门限参数。

硬阈值是指被检测数据所不能逾越的阈值;软阈值则是指被检测数据的变动范围。

在传输数据的稳定阶段,结点通过传感器不断地感知其周围环境。当结点首次检测到

数据到达硬阈值,便打开收发器进行数据传送,同时将该检测值存入内部变量 SV 中,结点再次进行数据传送时要满足两个条件:当前的检测值大于硬阈值;当前的检测值与 SV 的差异等于或大于软阈值。只要结点发送数据,变量 SV 便设置为当前的检测值,在簇重构的过程中,如果新一回合的簇首结点已经确定,该簇首将重新设定和发布以上 2 个参数。

TEEN 协议适合于需要实时感知的应用环境中,通过设置硬阈值和软阈值 2 个参数,TEEN 可以大大减少数据传送的次数,比 LEACH 节约能量。由于软阈值可以改变,监控者可以通过设置不同的软阈值可以方便地平衡监测准确性与系统节能指标。随着簇首结点的变化,用户可以根据需要重新设定 2 个参数的值,从而控制数据传输的次数。

TEEN 协议的缺点是不适合应用于需要周期性采集数据的应用系统中,这是因为如果网络中的结点没有收到相关的阈值,那么结点就不会与汇聚结点进行通信,用户也就完全得不到网络的任何数据。

7. SEC-Tree 协议

中国学者刘丹等人针对无线传感器网络的广泛应用及其对低能耗、高安全性迫切需求,提出了基于树的安全性和能量(Security and Energy Considering Tree,SEC-Tree)的拓扑结构。并以 SEC-Tree 拓扑结构为基础,设计了多层多路径路由协议,给出了一个自适应多路径路由算法。提出一种 PSK 密钥生成算法,并将 PSK 密钥应用于 SEC-Tree 初始化及路由维护中,实现了基于局部化的加密和鉴别技术,使该协议具有良好的安全特征、抗攻击能力和多跳、多路径路由的可靠特征。

为防止各类攻击,PSK 密钥在 WSN 路由邻接结点之间进行信息加密传送,在相邻结点相互身份鉴别之后才生成密钥,以提高网络安全性。具体步骤如下:

(1) 在网络初始化阶段,由可信任的接收中心(sink)生成主密钥 k^m,并配置给各个传感器结点。结点 i 根据主密钥生成自己的对称密钥 $k_i=f_k(i)$,其中 f_k 是伪随机函数。

(2) 结点对(I,j)在路由初始化时进行双向身份鉴别。

(3) 结点 i 给结点 j 发送请求身份鉴别消息包,其中包含自己的 ID 和消息认证码$\{i,\mathrm{MAC}(k_i,i)\}$;

(4) 结点 j 收到结点 i 的消息后,根据 i 计算出 k_i,并用其解密,完成对 i 的鉴别功能,鉴别成功则进入下一步,否则算法结束;

(5) 结点 j 给结点 i 发送确认信息,其中包含自己的 ID 和消息认证码$\{j,\mathrm{MAC}(k_j,j)\}$;

(6) 结点 i 收到 j 的应答信息后,根据 j 计算出 k_j,并用其解密,完成对 j 鉴别功能,鉴别成功则进入下一步,否则算法结束;

(7) 结点对(i,j)各自生成 i、j 间的 PSK 密钥:$k_{ij}=f_k(i)$;

(8) 各结点保留自己的密钥和 PSK 密钥,清除其他密钥,对于 i,保留密钥 k_i 和 k_{ij}。

SEC-Tree 对分层路由机制进行改进,将结点到簇头的数据交付修改为多跳交付机制,以减小数据传递的能耗,适应大规模 WSN 应用需求。同时,针对 SEC-Tree 的特性,设计自适应多路径安全路由策略,增强路由协议的抗攻击能力与容错能力,提高了可靠性。

8. GPSR 协议

贪婪边界无状态路由协议(Greedy Perimeter Stateless Routing,GPSR)是一种典型的

基于地理位置的路由协议，使用 GPSR 协议，网络结点都知道自身地理位置并被统一编址，各结点利用贪婪算法尽量沿直线转发数据。

GPSR 是使用地理位置信息实现路由(非辅助作用)的一种路由协议，它使用贪婪算法来建立路由。当结点 S 需要向结点 D 转发数据分组的时候，它首先在自己的所有邻居结点中选择一个距结点 D 最近的结点作为数据分组的下一跳，然后将数据传送给它。该过程一直重复，直到数据分组到达目的结点 D 或某个最佳主机。

产生或收到数据的结点向以欧氏距离计算出的最靠近目的结点的邻结点转发数据，但由于数据会到达没有比该结点更接近目的点的区域(称为空洞)，导致数据无法传输，当出现这种情况时，空洞周围的结点能够探测到，并利用右手法则沿空洞周围传输来解决此问题。该协议避免了在结点中建立、维护、存储路由表，只依赖直接邻结点进行路由选择，几乎是一个无状态的协议；且使用接近于最短欧氏距离的路由，数据传输时延小；并能保证只要网络连通性不被破坏，一定能够发现可达路由。

GPSR 协议的缺点是，当网络中汇聚结点和源结点分别集中在两个区域时，由于通信量不平衡易导致部分结点失效，从而破坏网络连通性；需要 GPS 定位系统或其他定位方法协助计算结点位置信息。

9. GEAR 协议

地理和能量感知路由协议(Geographic and Energy Aware Routing，GEAR)也是 Directed Diffusion 协议的一种改进，这种协议并不采用向整个网络广播的方式，而是利用地理位置信息，向某一特定区域发布数据包，该协议利用能量和地理位置信息作为启发式选择路径向目标区域传送数据。由于 GEAR 只向某个特定区域发送数据包，而不是像 DD 那样发布到整个网络，因此 GEAR 相对 Directed Diffusion 协议更加节省能量。

GEAR 协议的开销包括预估费用和修正费用两部分。预估费用是指结点剩余能量的费用和到目的结点的费用；修正费用则是对描述网络中环绕在空洞周围路由所需预估费用的修正，如果没有空洞现象的产生，那么预估费用等于修正费用。这里，空洞是指某个结点的周围的没有任何邻居结点比它自身更接近目标的区域。每当一个数据包成功到达目的地，该结点的修正费用就要传播到上一跳以便于对下一跳数据包的路由建立进行调整。

GEAR 协议的工作过程分为以下两个阶段。

1) 向目标区域传递数据包

当结点收到数据包时，首先要检查是否有邻居结点比它更接近目标区域。如果有，就选择距离目标区域最近的结点作为数据传递的下一跳结点。如果相对该结点来说，所有邻居都比它更远离目标区域，这就意味着该结点存在空洞现象。在这种情况下，利用修正费用选择其中的一个邻居结点来转发数据包。

2) 在目标区域内广播数据包

如果数据包已经到达目标区域，可以利用递归的地理传递方式和受限的 Flooding 方式发布该数据包。当传感器结点的分布不太紧密时，受限的 flooding 方式是比较好的选择。而在高密度的无线传感器网络内，递归的地理传递方式相对受限的 flooding 方式更加节能。在这种情况下，目标区域被划分为 4 个子区域。数据包也相应地被复制了 4 次，这种分割和数据传递过程不断重复，直到区域内只剩下一个结点为止。

10. TBF 协议

临时数据块流协议(Temporary Block Flow,TBF)是一种基于源结点和位置的路由协议。与通常的基于源结点的路由协议不同,TBF 协议利用参数在数据包的头部中指定一条连续的传输轨道,而不是路由结点序列;与前面介绍的基于位置的 GPRS 路由协议不同,TBF 协议也不是沿着最短路径传播数据的。

临时数据块流是指两个无线资源实体所使用的一个数据块流,以达到在分组数据信道(Packet Data CHannel,PDCH)上支持单向传递逻辑链路控制协议数据单元(Logical Link Control Protocol Data Unit,LLC PDU)的目的。网络可以给 TBF 分配一个或多个 PDCH 信道。一个 TBF 包含很多 RLC/MAC 块,用来承载一个或多个 LLC PDU。

网络给每一个 TBF 安排一个临时数据块标识(Temporary Flow Indicator,TFI),用来唯一的标识一个 TBF。在上行链路方向,TBF 协议使用上传状态标记(Uplink Status Flag,USF),从而允许不同的移动站点(Mobile Site,MS)动态复用一个无线数据块。USF 包含在下行 RLC/MAC 块的块头内,当 MS 收到一个下行 RLC/MAC 块内的 USF 值与之前分配给移动站点的 USF 值相同时,MS 就准备在上行链路的对应时隙进行上行 RLC/MAC 块的传递。

TBF 协议主要有以下几个特点:可利用 GPRS 协议的方法或其他方法避开空洞;通过指定不同的轨道参数,容易实现多路径传播和广播、对特定区域的广播和多播;允许网络拓扑变化,可避免传统源站路由协议的缺点。现代网络发展中的不利因素主要是:随着网络规模变大,路径加长,沿途结点进行计算的开销也相应增加;且需要 GPS 定位系统或其他定位方法协助计算结点位置信息。

4.2.10 无线传感器网络密钥管理机制

在所有的无线传感器网络的安全解决方案中,加密技术是一切安全技术的基础。通过加密技术可以满足感知信息认证、机密性、不可否认性、完整性等安全需求。对于加密技术来说,密钥管理是其中最关键的一个因素。

针对无线传感器网络的特点,近年来研究者们已经提出了许多关于密钥管理的方案,但这些方案都有自己不同的侧重点和优缺点。本节从无线传感器网络的安全角度入手,分别对各种方案的计算复杂度、结点被俘后网络的恢复能力、网络的扩展性和支持的网络规模等方面进行分析,讨论各种适合无线传感器网络的典型密钥管理方案的优缺点。

由于无线传感器网络面临特殊的安全威胁,因此传统的网络密钥管理方案已经不再适合于无线传感器网络。针对其特殊性,目前已经提出多种密钥管理方案,包括分布式密钥管理方案(如预置所有对密钥方案、随机密钥预分配方案等)和分簇式密钥管理方案(如低能耗密钥管理方案、轻量级密钥管理方案等)。

1. 分布式的密钥管理方案

在分布式的无线传感器网络中,没有固定基础设施,网络结点之间的能量和功能都是相同的。当部署分布式的网络时,将结点随机地投掷到目标区域,各结点自组织地形成网络,其网络结构如图 4-13 所示。

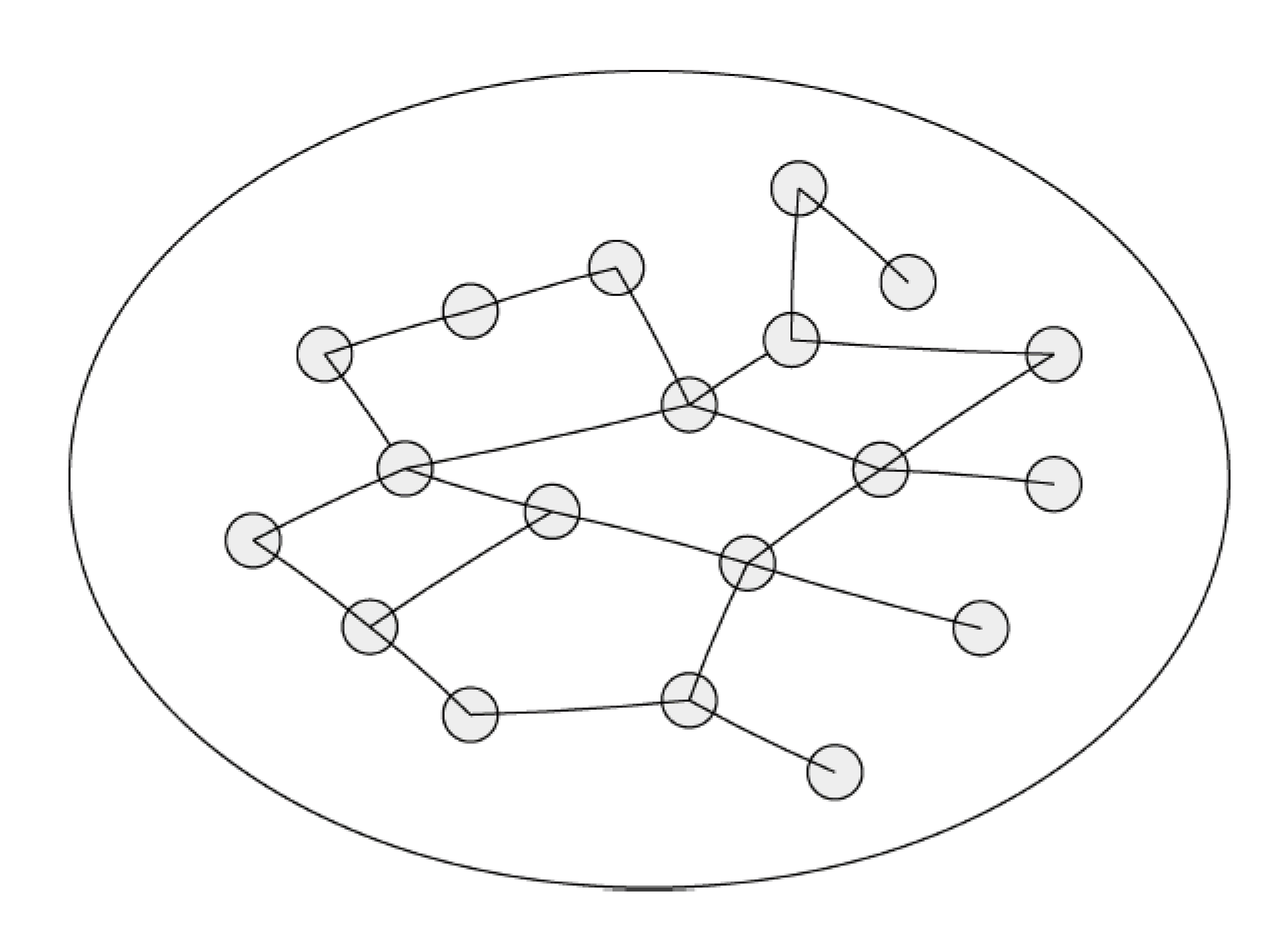


图 4-13　分布式无线传感器网络体系结构

目前，已经提出了多种分布式的密钥管理方案。例如预置全局密钥的方案、预置所有结点对密钥的方案和随机预分配密钥的方案等。

1）预置全局密钥的方案

在 TinyOS 系统的 TinySec 中便采取了这种安全机制，它是最简单的密钥建立过程。所有的传感器结点预配置一个相同的密钥，所有的结点均利用该密钥进行加密、解密、认证以及密钥的协商和更新。这种方案的优点是计算复杂度低，由于网络中只有一个密钥，所以很容易增加新的结点；缺点是网络的安全性较差，任何一个结点被俘获就会导致整个网络瘫痪。

2）预置所有结点对密钥的方案

预置所有结点对密钥的密钥管理方案是由 Bocheng 等人提出的。其主要思想是每对结点之间共享一对密钥，以保证每对结点间的通信都可以使用预配置的共享密钥加密，其要求每个结点存储的对密钥数为 $n-1$ 个（n 为网络结点总数）。该方案的优点是不依赖于基站，灵活性比较强，计算复杂度低，任意两个结点间的密钥是独享的，所以当一个结点被俘获后不会影响网络中其他结点通信的安全性；缺点是支持网络的规模小，因为传感器结点的存储量有限，当网络中结点数目足够大的时候，$n-1$ 个密钥的存储量将大大地超过结点的存储量，可扩展性不好，不支持新结点的加入。

3）随机密钥预分配方案

随机密钥预分配方案是由 Eschenauer 和 Gligor 等人最早提出的，其主要思想是从预置所有对密钥方案改进的。它将预存网络中的所有对密钥改为预存部分密钥，减小了对结点资源的要求。随机密钥预分配的具体实施过程如下：

（1）密钥的产生。

首先产生一个大的密钥池 S，并为每个密钥分配一个标识符 ID(Identity)，然后从密钥池 S 中随机选取 K 个密钥存入结点的存储器里，K 个密钥称为结点的密钥环。K 的选择应保证每两个结点之间至少拥有一个共享密钥的概率大于一个预先设定的概率 P。

（2）共享密钥的发现。

每个结点广播自己密钥链中所有密钥的标识符 ID，找出位于自己通信范围内的与自己

有共享密钥的结点。共享密钥发现阶段建立了结点排列的拓扑结构，当两个结点间存在共享密钥时，这两个结点间就存在一个连接，通过链路加密所有基于该连接的通信都是安全的。

(3) 路径密钥的建立。

结点和那些与自己没有共享密钥的邻居结点通过已有的安全连接协商路径密钥，以后这些结点之间就可以通过路径密钥建立安全连接。

当检测到一个结点被俘获时，为了有效地删除结点的密钥链，控制结点广播被俘结点所有密钥的标识符 ID，其他结点收到信息后删除自己密钥链中含有相同标识符 ID 对应的密钥。一旦密钥从密钥链上删除，与删除的密钥相关的连接将会消失，受影响的结点需要重新启动共享密钥发现以及路径密钥的建立。这种方案的优点是计算复杂度比较低，网络具有一定的扩展能力，实现简单；缺点是对部分结点被俘获的抵抗性太差，攻击者可以通过交换的标识符 ID 分析出网络的安全连接，从而攻破少数的结点而获取较大份额的密钥，从而影响其他结点间的通信。

Chan 等人在 Eschenauer 和 Gligor 方案的基础上，又提出了 Q2 composite 随机密钥预分配方案，该方案将任意两个相邻结点间的共享密钥数提高到 q 值。通过提高 q 值增强了网络对结点攻击的抵抗性，缺点是密钥的重叠度增加，限制了网络的可扩展性。

此外，还有基于多项式的随机密钥预配置方案，如 Polynomial Pool Based Key Scheme 和 Location 2 Based Pair 2 Wise Establishments Scheme 密钥管理方案，这些方案能有效地抵抗部分结点被俘获后对网络安全造成的影响，只有当敌手获取了同一多项式的 t 项才能计算出多项式。网络的可扩展性较好，可以支持大规模的网络；但需要的计算开销太大，由于结点的计算能力有限，因此需要对算法作进一步的优化。

2. 分簇的密钥管理方案

在分簇式无线传感器网络结构中，根据各个结点的功能和能量不同，可以将结点分成三类：基站、簇头和普通的传感器结点，其体系结构如图 4-14 所示。

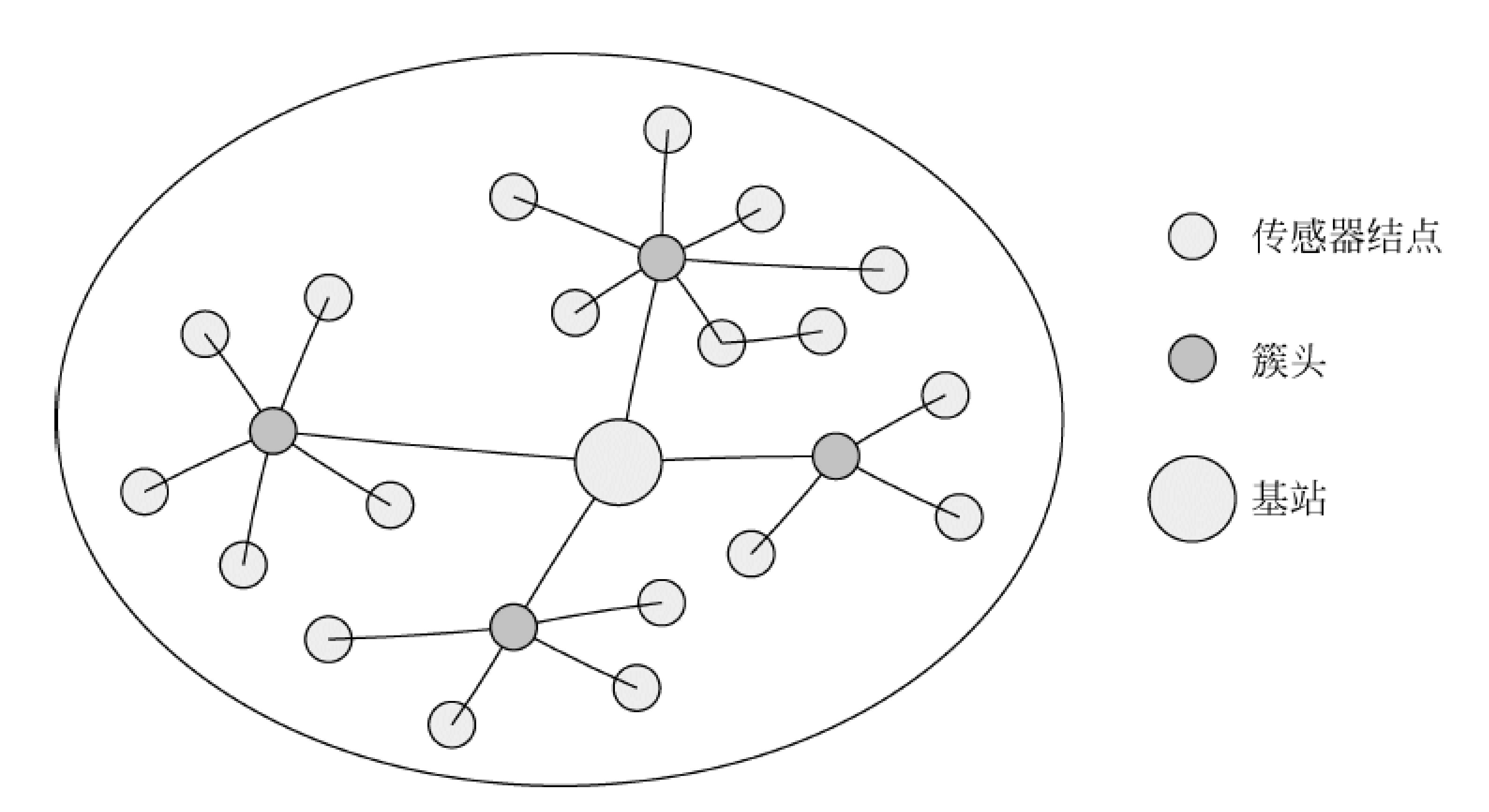


图 4-14 分簇式无线传感器网络体系结构

在网络中基站的能量和存储能力是不受限制的，它主要负责收集和处理传感器结点发送来的数据以及管理整个网络。

在大多数的应用中，假定基站是安全的、可以信任的，因此把基站用来作密钥服务器。相对于传感器结点，簇头拥有较高的信息处理和存储能力，它负责将结点分簇、收集并处理来自结点的信息然后将信息发送给基站。在部署网络时，传感器结点被随机地投掷在目标区域，随后结点搜寻自己无线范围内的临近簇头自组织形成网络。针对分簇式网络现已提出了低能耗密钥管理和轻量级密钥管理等方案。

1）基于密钥颁发中心（Key Distribution Center，KDC）的结点对密钥管理方案

基于密钥颁发中心的结点对密钥管理方案的基本思想，是每个传感器结点与 KDC 共享一个密钥，在这里基站可以作为 KDC。KDC 保存与所有结点的共享密钥，如一个结点要与另一个结点通信，它需要向 KDC 发出请求，然后 KDC 产生会话密钥，并将其传给相应的结点。这种方案的优点是计算复杂度低，对结点存储和计算能力要求不高，网络有很好的自恢复能力，部分结点被俘获不会影响到网络其他结点的通信；缺点是网络的可扩展性与支持的网络规模取决于基站的能力，网络通信过分依赖基站，如基站被俘整个网络就被攻破。

2）低能耗密钥管理方案

低能耗的密钥管理方案是由 Jolly 等人提出来的，它是基于 IBSK 协议的扩展，继承了 IBSK 支持增加、删除结点以及密钥更新的优点，同时为了减少能量的消耗，取消了结点与结点之间的通信。由于目前一些技术的不成熟，所以该协议是在一些假设的基础上进行的。首先假定基站有入侵检测机制，可以检测出结点的正常与否，并由此决定是否触发删除结点的操作；对传感器结点不作任何信任的假设，簇头之间可以通过广播或单播与结点通信。在网络部署前，分配给每个传感器结点两个密钥，一个与簇头共享，一个与基站共享，所有簇头共享一个密钥用于簇头间的广播通信，每个簇头还分配有一个与基站共享的密钥和随机指定的 $|S|/|G|$ 个传感器结点的密钥（$|S|$ 为传感器结点的个数，$|G|$ 为簇头的个数）。在簇形成阶段，结点广播用与簇头共享的密钥加密后的自己的位置和能量的信息，簇头收到该信息后与其他簇头交换属于自己通信范围内结点的密钥，密钥交换完成后簇头指定自己通信范围内的结点形成簇。增加新的结点时，首先基站随机选取一个簇头，将新结点的密钥发送给该簇头，然后通过簇形成阶段，新结点就加入了该簇。该方案的优点是对结点的存储和计算能力要求不高，由于预存了所有密钥，计算复杂度也较低，网络的自恢复能力强；缺点是网络的可扩展性不高，通信过于依赖簇头，多个相邻簇头的被俘可能导致整个网络的瘫痪。当删除簇头时，方案中要给出一个指定的新簇头，然后将旧簇内的结点分配给新簇头。这种思想在实际应用中是不可行的，因为不能保证重新部署的新的簇头正好位于旧簇头的位置上，也就不能保证新的簇头能涵盖旧簇头内所有的结点。

3）轻量级密钥管理方案

Eltoweissy、Younis 和 Ghumman 等人也提出了轻量级密钥管理方案，这个方案采用了组合最优组 EBS（Exclusion Basis System）密钥的算法，用于密钥的分配与更新。在网络部署前每个传感器结点预配置唯一的 ID 标识符和两个密钥，这两个密钥一个与簇头共享，另一个与基站共享。当簇头被俘获后，通过与基站共享的密钥，结点可以重新获得新的簇头与密钥。簇头预配置一个与基站共享的密钥和唯一的 ID 标识符，且假定其有一定入侵检测的能力；密钥只能由基站产生且也假定其具有入侵检测的能力。

在网络的初始化阶段，簇头广播自己的信息，基站在收到簇头的信息后，根据簇头的数目构建 EBS 并发送信息给簇头，该信息包括管理密钥和簇头间的会话密钥。在簇的形成阶

段,结点发送自己的ID和位置信息,簇头接收到后将结点的ID和位置信息制成表,与其他簇头协商形成簇,簇头最后根据簇内结点的数目决定需要的密钥数并将需要的密钥数和结点的标识符列表发送给基站。基站产生需要的密钥并据此为每个簇构建EBS,并将信息传给簇头,最后由簇头指定结点的归属。当检测到簇头被俘获时,首先将簇头从网络中删除,然后依靠其他正常的簇头确认那些孤立的传感器结点,并将在自己通信范围内的结点加入簇内。

轻量级密钥管理方案的主要优点,是引入了组播的概念和组播密钥管理算法。利用EBS较好地实现了密钥的产生、分配及密钥的更新,有效地保护了当前、前向与后向秘密;网络的可扩展性较好,可以支持大规模的网络,可以支持网络的动态变化,单个结点的俘获对网络的安全通信影响不大。缺点是当结点频繁地被俘获时,频繁的密钥更新大大增加了网络的通信负载。但是该方案也没有很好地解决删除簇头后簇内结点的分配问题,这是在分簇的密钥管理方案中普遍存在的问题,也需要对分簇算法作进一步优化。

4.3 物联网终端安全

物联网终端是物联网中连接传感器网络,实现采集物理世界中的原始数据并向物联网发送数据的终端设备。它担负着数据采集、初步处理、加密和传输等多种功能。

4.3.1 物联网终端概述

1. 物联网终端的工作原理

物联网终端由外围感知接口(传感器接口)、中央处理模块和外部通信接口等三个部分组成,通过外围感知接口与传感设备连接,如RFID读卡器、红外感应器和环境传感器等。对这些传感设备的数据进行采集并通过中央处理模块处理后,按照网络协议,经过外部通信接口,如GPRS模块、以太网接口和Wi-Fi等方式发送到以太网的指定中心处理平台。

物联网终端属于传感网络层与传输网络层的中间设备,也是物联网的关键设备。通过物联网终端的转换和采集,才能将各种外部感知数据加以汇集和处理,并将数据通过各种网络接口方式传输到互联网中。如果没有物联网终端,传感数据将无法送到指定位置,“物”联网将不能实现。

2. 物联网终端的分类

1) 按传输方式分类

物联网终端按传输方式来分类,可以分为以太网终端、Wi-Fi终端、2G终端、3G和4G终端等,有些智能终端同时具备多种终端的功能。

(1) 以太网终端。

这类终端一般应用在数据传输量比较大、以太网条件较好的场合,终端现场很容易布线并具有连接互联网的条件。以太网终端一般应用在工厂的固定设备检测、智能大厦和智能家居等环境中。

(2) Wi-Fi 终端。

这类终端一般应用在数据传输量较大、以太网环境比较好,但是终端部分布线不容易或者不能布线的场合,在终端周围架设 Wi-Fi 路由或 Wi-Fi 网关等设备来实现。Wi-Fi 终端一般应用在无线城市和智能交通等需要大数据无线传输的场合,或其他应用终端周围不适合布线,但需要大量数据传输的场合。

(3) 2G 终端。

这类终端应用在小数据量传输的移动场合和小数据量传输的野外工作场合,例如物流 RFID 手持终端、车载 GPS 定位、河流水位监测、水库水质监测和空气质量监测等。这类终端因为具有移动中或野外条件下的联网功能,所以为物联网的深层次应用提供了更加广阔的市场。

(4) 3G 和 4G 终端。

这类终端是在 2G 终端基础上进行升级,采用 3G 甚至 4G 通信技术,可以大大提高上行、下行的通信速率,以满足移动图像监控和传输视频等应用场合,例如巡警图像回传、动态实时交通信息的监控等,在一些大数据量的传感应用中,如地震波信号的采集和电力信号实时监测中也可以用到该类终端。

2) 按行业应用分类

物联网终端按行业应用来分类,可以分为工业设备检测终端、农业设施检测终端、物流 RFID 识别终端、电力系统检测终端和安防视频监控终端等。

(1) 工业设备检测终端。

这类终端主要安装在工厂的大型设备上或工矿企业的大型运输机械上,用来采集位移传感器、位置传感器,振动传感器、液位传感器、压力传感器和温度传感器等数据,通过终端的有线网络或无线网络接口,发送到中心处理平台进行数据的汇总和处理,实现对工厂设备运行状态的及时跟踪和大型机械的状态确认,达到安全生产的目的。抗电磁干扰和防暴是这类终端设计的重点。

(2) 农业设施检测终端。

这类终端一般被安装在位于大棚或温室中的农业设施上,主要用于采集空气温度和湿度传感器、土壤温度传感器、土壤水分传感器、光照传感器和气体含量传感器的数据,将数据打包、压缩和加密后,通过终端的有线网络和无线网络接口发送到中心处理平台进行数据的汇总和处理。这种系统可以及时发现农业生产中不利于农作物生长的环境因素,并在第一时间通知管理者纠正这些因素,从而提高农作物的产量,减少病虫害发生的概率。防水、防晒和防腐设计是这类终端设计的重点。

(3) 物流 RFID 识别终端。

这类终端可以分为手持式、固定式和车载式。手持式 RFID 识别终端由使用者手持使用;固定式 RFID 识别终端一般安装在仓库门口或其他货物通道;车载式 RFID 识别终端安装在物流运输车中。固定式一般只有识别功能,用于跟踪货物的出库和入库;手持式和车载式一般具有 GPS 定位功能和基本的 RFID 标签扫描功能,用来识别货物的状态、位置和性能等参数,通过有线或无线网络将位置信息和货物的基本信息传送到中心处理平台。通过该类终端的货物状态识别,可以将物流管理变得非常方便,大大提高了物流的效率。

3）按使用场合分类

按使用场合分类，物联网终端可以分为固定终端、移动终端和手持终端。

（1）固定终端。

这类终端应用在固定场合，一般固定不动，具有可靠的外部电源供电和可靠的有线数字链路，用于监测各种固定设备、仪器或环境的信息，工业设备和农业设施用的监测终端均属于此类。

（2）移动终端。

这类终端应用在终端与检测设备同时移动的场合。由于该类终端经常发生运动，因此没有可靠的外部电源，需要通过无线数据链路进行数据的传输，主要用于检测如图像、位置、运动设备的某种物理状态。车载视频监控设备、车载仪器和货物 GPS 定位等均使用这类终端。这类终端一般要求具备良好的抗震和抗电磁干扰能力，对供电电源的要求也比较高。

（3）手持终端。

这类终端是在移动终端的基础上进行了升级和改造，它一般小巧轻便，使用者可以随身携带，有后备电池，一般可以连续使用 8 小时以上。具有可以连接外部传感设备的接口，采集的数据一般可以通过无线进行及时传输，也可以在积累一定程度后通过有线传输。这类终端大部分应用在物流 RFID 识别、工厂设备参数巡检和农作物病虫害普查等领域。

4）按使用扩展性分类

物联网终端按使用扩展性分类，可以分为单一功能终端和通用智能终端两类。

（1）单一功能终端。

这类终端一般外部接口较少，设计简单，仅满足单一应用或者单一应用的部分扩展。除了这种应用以外，必须修改硬件才能应用在其他场合。目前市场上这一类终端比较多，例如汽车监控用的图像传输服务终端、电力监测用的终端和物流用的 RFID 终端等。这些终端功能单一，仅适用于特定场合，不能随应用变化进行功能改造和扩充。由于功能单一，这一类终端的成本比较低，也比较容易标准化。

（2）通用智能终端。

这类终端因为考虑了行业应用的通用性，所以外部接口比较多，设计复杂，能满足两种或者两种以上场合的应用。通用智能终端可以通过内部软件的设置、修改应用参数或者通过硬件模块的装卸，来满足不同的应用需求。这类硬件模块一般涵盖了大部分应用对接口的需求，并具有网络连接的有线或者无线的多种接口方式，还可以扩展蓝牙、Wi-Fi 和 ZigBee 等接口，甚至预留一定的输出接口用于物联网应用中对“物”的控制。这类终端开发难度比较大，成本比较高，仍然没有标准化，目前市场上这一类终端很少。

5）按传输通路分类

物联网终端按照传输通路来分类，可以分为数据透传终端和非数据透传终端。

（1）数据透传终端。

数据透传终端在输入口与应用软件之间建立起数据传输通路，使得数据可以通过模块的输入口输入，通过软件原封不动的输出，表现给用户的方式相当于一个透明的通道，因此称为数据透传终端。目前这一类终端在物联网集成项目中得到了大量应用。其优点是很容易构建出符合应用需求的物联网系统，缺点是功能单一。在多路数据或者多类型数据传输时，需要使用多个采集模块进行数据的合并处理后，才可以通过这一类终端传输；否则每一

路数据都需要一个数据透传终端,这样会大大增加成本和系统的复杂程度。目前市场上的大部分通用终端都属于数据透传终端。

(2)非数据透传终端。

这一类终端一般将外部多个接口的采集数据通过终端内部的处理器合并后传输,因此具有多路同时传输的优点,同时减少了终端的数量。其缺点是只能根据终端的外围接口选择应用,如果满足所有应用,该终端的外围接口种类就需要很多。在不太复杂的应用中会造成很多接口资源的浪费,因此接口的可插拔设计是此类终端的共同特点,前文提及的通用智能终端就属于此类终端。数据传输应用协议在终端内已经集成,作为多功能应用,通常需要提供二次开发接口。目前市场上这一类终端较少。

6)按应用对象分类

物联网终端按照应用对象分类,可以分为感知识别型终端和应用型终端。

(1)感知识别型终端。

感知识别型终端主要针对外部世界环境参数的采集,以二维码、RFID传感器为主,实现对"物"的识别或者环境状态的感知。

(2)应用型终端。

应用型终端主要针对人的应用,提供键盘、鼠标、触摸屏和显示器等各种输入输出接口,例如计算机、平板电脑和智能手机等都属于此类终端。

特别值得注意的是,近几年来快速普及的智能手机可以说是一种随身携带的超级感知和识别设备。智能手机上可以配备的传感器种类繁多,例如加速度传感器、陀螺仪传感器、温度传感器、方向传感器、压力传感器、距离传感器、光线亮度传感器等。智能手机还具备GPS定位功能,可以提供基于位置的服务。智能手机上摄像头的拍照功能也是感知声音、图像、影像能力的体现。如果把RFID标签附着在手机内部,手机就具有了标示手机主人的功能。在智能手机触摸屏安装RFID读写器,手机便具有标签读取功能,可以通过读取RFID标签来识别物体。

4.3.2 嵌入式系统安全

1. 嵌入式系统的安全架构

物联网的感知识别型终端系统通常是嵌入式系统。嵌入式系统是以应用为中心,以计算机技术为基础,并且软硬件是可订制的,适用于对功能、可靠性、成本、体积和功耗等有严格要求的专用计算机系统。嵌入式系统的发展过程,经历了无操作系统、简单操作系统、实时操作系统和面向互联网的操作系统等四个阶段。

结合嵌入式信息系统的结构,以下分别从硬件平台、操作系统和应用系统等三个方面对嵌入式系统的安全性进行分析。

1)硬件平台的安全性

为适应不同应用功能的需要,嵌入式系统采用多种多样的系统结构,攻击者可能采用的攻击手段也呈现多样化的趋势。区别于个人电脑系统,嵌入式信息系统可能遭到的攻击存在于系统体系结构的各个部分。

(1)对可能发射的各类电磁信号的嵌入式系统,利用其传输和辐射的电磁波,攻击者可

能使用灵敏的测试设备进行探测、窃听、甚至拆卸,以便提取数据,导致电磁泄露攻击或者侧信道攻击。而对于嵌入式存储元件和移动存储卡,存储部件内的数据也容易被窃取。

(2)针对各类嵌入式系统传感器、探测器等低功耗敏感设备,攻击者可能引入极端温度、电压偏移和时钟变化,从而强迫系统在设计参数范围之外工作,表现出异常性能。特殊情况下强电磁干扰和电磁攻击,则可能将毫无物理保护的小型嵌入式系统彻底摧毁。

2)操作系统的安全性

与个人电脑不同的是,嵌入式产品采用数十种体系结构和操作系统,常用的嵌入式操作系统包括 Windows CE、VxWorks、pSOS、QNX、PalmOS、OS-9、LynxOS、Linux 等,这些系统的安全等级各不相同,但是各类嵌入式操作系统都普遍存在因为硬件平台计算能力和存储空间有限,所以精简代码而牺牲系统安全性的情况。嵌入式操作系统普遍存在的安全隐患如下:

(1)由于系统代码的精简,对系统的进程控制能力并没有达到一定的安全级别。

(2)由于嵌入式处理器的计算能力有限,缺少系统的身份认证机制,攻击者可能轻易破解嵌入式操作系统的登录口令。

(3)大多数嵌入式系统的系统文件和用户文件缺乏必要的完整性保护机制。

(4)嵌入式操作系统缺乏数据的备份和可信恢复机制,系统一旦发生故障便无法恢复。

(5)各种嵌入式信息终端病毒正在不断出现,并大多通过无线网络注入终端。

3)应用软件的安全性

应用软件的安全问题普遍存在,其中包括应用层安全问题(如病毒、恶意代码攻击等)、中间件安全问题和系统层安全问题(如数据窃听、源地址欺骗、源路由选择欺骗、鉴别攻击、TCP 序列号欺骗、拒绝服务攻击等)。

2. 嵌入式系统的安全机制

嵌入式系统的安全机制可以根据嵌入式系统不同层次的安全需求来制定,嵌入式系统的分层安全对策如图 4-15 所示,以下分别从下层至上层进行简要分析。

安全应用层(应用程序、网络安全协议等)
软件安全架构层(操作系统、虚拟机等)
硬件安全架构层(CPU、内存、加密芯片等)
安全电路层(电路元件、封装等)

图 4-15 嵌入式系统的分层安全对策

1)安全电路层

通过对传统的电路加入安全措施和改进设计,实现对涉及敏感信息的电子器件的保护。可以在安全电路层采用的措施包括:通过降低电磁辐射、加入随机信息等来降低非入侵攻击所能测量到的敏感数据特征;加入开关、电路等对攻击进行检测,例如用开关检测电路的物理封装是否被打开。在关键应用如工业控制中还可以使用容错硬件设计和可靠性电路设计。

2)硬件安全架构层

这种方法借鉴了可信平台模块(Trusted Platform Module,TPM)的思路,采取的措施

包括：加入部分硬件处理机制以支持加密算法甚至安全协议；使用分离的安全协议处理器模块以处理所有敏感信息；使用分离的存储子系统作为安全存储空间，这种隔离可以限制存取权限，只有可靠的系统部件才可以对安全存储区间进行存取；如果上述功能不能实现，可以利用存储保护机制，即通过总线监控硬件来区分对安全存储区域的存取是否合法来实现，对经过总线的数据在进入总线前进行加密以防止总线窃听。典型的例子包括 ARM 公司的 Trustzone 和 Intel 公司的 LaGrande 等。

3）软件安全架构层

软件安全架构层主要通过增强操作系统和虚拟机的安全性来增强系统安全的，例如微软公司的下一代安全计算基础（Next-Generation Secure Computer Base，NGSCB），通过与相应硬件的协同工作提供如下增强机制：进程分离（用来隔离应用程序，免受外来攻击）；封闭存储（让应用程序安全地存储信息）；安全路径（提供从用户输入到设备输出的安全通道）；认证证书（用来认证软硬件的可信性）。其他方法还有通过加强 Java 虚拟机的安全性，对非可靠的代码使其在受限制和监控的环境中运行。另外，该层还对应用层的安全处理提供必要的支持。例如，在操作系统之内或之上充分利用硬件安全架构的硬件处理能力优化和实现加密算法，并向上层提供统一的应用编程接口等。

4）安全应用层

通过利用下层提供的安全机制，实现涉及敏感信息的安全应用程序，保障用户数据安全。这种应用程序可以是包含诸如提供 SSL 安全通信协议的复杂应用，也可以是仅仅简单查看敏感信息的小程序，但必须符合软件安全架构层的结构和设计要求。

4.4 本章小结

射频识别（Radio Frequency Identification，RFID）是一种非接触式自动识别技术。它通过无线射频方式自动识别特定目标的标签，并读写标签中的相关信息。

一套完整的 RFID 系统，通常由物理世界（Physical World）、电子标签（Tag）、天线（Antenna）、读写器（Reader and Writer）、中间件（Middleware）和应用软件（Application Software）等部分组成。

RFID 标签俗称电子标签，也称为应答器（Tag、Transponder 或 Responder），根据工作方式可分为主动式（有源）标签和被动式（无源）标签两大类。

被动式 RFID 标签由标签芯片和标签天线或线圈组成，利用电感耦合或电磁反向散射耦合原理实现与读写器之间的通信。

天线（Antenna）是 RFID 标签和读写器之间实现射频信号空间传播和建立无线通信连接的设备。

读写器（Reader）也称为读写器或询问器（Interrogator），是对 RFID 标签进行读/写操作的设备，主要包括射频模块和数字信号处理单元两部分。

中间件（Middleware）是一种面向消息的、可以接受应用软件端发出的请求、对指定的一个或者多个读写器发起操作并接收、处理后向应用软件返回结果数据的特殊软件。

应用系统（Application System）使用位于后台的数据库管理系统来实现其管理功能，是直接面向 RFID 应用最终用户的人机交互界面，协助使用者完成对读写器的指令操作以及

对中间件的逻辑设置,逐级将 RFID 原子事件转化为使用者可以理解的业务事件,并使用可视化界面进行展示。

一套完整的 RFID 系统的工作原理是读写器(Reader)发射一特定频率的无线电波能量给 Transponder,用以驱动 Transponder 电路将内部的数据送出,此时 Reader 便依序接收解读数据,送给应用系统作相应的处理。

当电子标签进入磁场后,读写器发出射频信号,电子标签凭借天线感应电流所获得的能量,发送出存储在芯片中的产品信息(Passive Tag,无源标签或被动标签),或者由电子标签主动发送某一频率的信号(Active Tag,有源标签或主动标签),读写器读取信息并解码后,送至中间件进行有关数据处理。

一套比较完美的 RFID 系统安全解决方案,应当具备机密性、完整性、可用性、真实性和隐私性的基本特征。

RFID 系统一般由电子标签、天线、读写器、中间件、应用系统等部分组成。对于攻击者来说,这几个部分都可能成为攻击的目标。

针对标签和读写器的攻击手段包括窃听、略读、克隆、重放、追踪、扰乱系统等;针对应用系统和后台数据库的攻击则包括标签伪造与复制、ONS 攻击、病毒攻击等。

实现 RFID 系统安全性所采用的安全机制分为三大类:物理安全机制、密码安全机制以及两者相结合的机制。

物理安全机制通常用于低成本标签中,因为这些标签难以采用复杂的密码机制来实现与读写器之间的安全通信。物理机制主要包括五大类:Kill 命令机制、休眠机制、阻塞机制、静电屏蔽和主动干扰等。

密码安全机制是指利用各种成熟的加密算法和安全机制,来设计和实现符合 RFID 系统的安全需求。RFID 系统的信息系统安全是物联网研究的热点之一,近年来,研究者们提出了很多低成本的安全认证协议,例如 hash-lock(哈希锁)协议、随机化 hash-lock(随机化哈希锁)协议、hash-chain(哈希链)协议、Hash 函数构造算法、基于矩阵密钥的认证协议、数字图书馆协议等。

无线传感器网络(Wireless Sensor Networks,WSN)是由部署在监测区域内大量的廉价微型传感器结点组成,并通过无线通信方式形成的一个多跳的、自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中被感知对象的信息,并发送给观察者。

无线传感器网络的发展历程共经历了三个阶段:传感器→无线传感器→无线传感器网络(大量微型、低成本、低功耗的传感器结点组成的多跳无线网络)。

在各种无线传感器网络中,传感器数据采集及传输常用的方式主要有周期性采样、事件驱动和存储与转发。实现其技术的网络结构也有 3 种:星型网、网型网和混合网(星型网+网型网)。每种网络都有各自的优点及缺点,用户应当充分了解这些网络的特点以满足不同应用的实际需要。

无线传感器网络的特点包括:大规模、自组织、动态性、可靠性、以数据为中心、集成化、具有密集的结点布置、以协作方式执行任务、结点唤醒方式。

由于无线传感器的资源有限,网络往往运行在十分恶劣的环境中,因此很容易受到恶意攻击。无线传感器网络面临的安全威胁与传统移动网络相似。无线传感器网络的安全威胁主要包括:干扰、截取、篡改、假冒。

网络系统安全需求的目标是要保证网络中传输信息的安全性。无线传感器网络中的信息安全需求主要包括：机密性、完整性、真实性、可用性、新鲜性、鲁棒性、访问控制。

为了实现无线传感器网络的安全需求，必须同时采取多种不同的安全技术。设计并实现通信安全一体化的无线传感器网络协议栈，是实现安全无线传感器网络的关键。安全一体化的网络协议栈能够从整体上应对无线传感器网络面临的各种安全威胁，达到满意的效果。安全一体化的网络协议栈通过整体设计、优化设计将传感器网络的各类安全问题统一解决，包括认证、密钥管理、安全路由等。

为了保证结点的物理层安全，必须解决结点的身份认证和通信问题。应研究使用合适的天线来解决结点间的通信，保证各个结点间及基站与结点间可以有效地互相通信。研究多信道问题，防范针对传感器结点的物理攻击。

为加强物理层的保护，可以在传感器结点加入配置防篡改模块（Tamper Proof Module，TPM），该模块允许安全地存储证书，当传感器结点受到威胁时阻止攻击者检索证书，一旦发现针对传感器的篡改行为，配置防篡改模块就会实施自销毁，破坏存储在模块中的所有数据和密钥。在拥有足够冗余信息的传感器网络中，这是一种切实可行的解决方案。

针对外部存储器的读取攻击，一种可行的应对措施是对外部存储器进行定期检查，对断开微控制器和外部存储器的时间设置严格的约束。

媒体访问控制协议（Media Access Control，MAC）处于传感器网络的底层，对传感器网络的性能有较大的影响，是保证无线传感器网络高效通信的关键网络协议之一。无线传感器网络的 MAC 协议是由传统的 CSMA 协议改进而来，典型的协议有 S-MAC、SMACS/EAR、T-MAC、DMAC 等。

SPINS 安全体系是目前研究者提出的传感器网络安全体制中比较流行、实用的无线传感器网络安全方案。它在数据机密性、完整性、新鲜性、可认证等方面都做了充分的考虑。

SPINS 安全协议包含 SNEP（Security Network Encryption Protocol）和 μTESLA（micro Timed Efficient Streaming Loss-tolerant Authentication）两个部分。SNEP 用以实现通信的机密性、完整性、新鲜性和点到点的认证；μTESLA 用以实现在资源受限情况下的点到多点的广播认证。

无线传感器网络路由协议的设计是一个技术难题，网络中所有结点都应可达（连通性），网络结点还要求尽量大地覆盖目标区域，要容许网络中部分结点由于能量或别的原因无法正常工作。路由算法也要能适应不同的网络规模和结点密度，并要具有一定的服务质量要求。除了低存储器容量、低功耗，安全也是不可忽略的重要因素。

目前，适用于无线传感器网络中的路由协议有许多，大致可以分为三类：以数据为中心的路由协议、层次式路由协议和基于位置的路由协议。

典型的单层无线传感器网络路由协议包括 SPIN 协议、Directed Diffusion 协议和谣言协议等。

典型的多层路由协议包括 LEACH 协议、PEGASIS 协议、TEEN 协议和 SEC-Tree 协议等。

典型的基于地理位置的路由协议包括 GPSR 协议、GEAR 协议和 TBF 协议等。

在所有的无线传感器网络安全解决方案中，加密技术是一切安全技术的基础，通过加密可以满足感知信息认证、机密性、不可否认性、完整性等安全需求。对于加密来说，密钥管理

是其中最关键的问题。

由于无线传感器网络面临特殊的安全威胁,因此传统的密钥管理方案已经不再适合于无线传感器网络。针对其特殊性,现已提出许多相应的密钥管理方案,主要有分布式密钥管理方案(如预置所有对密钥方案、随机密钥预分配方案等)和分簇式密钥管理方案(如低能耗密钥管理方案、轻量级密钥管理方案等)。

物联网终端是物联网中连接传感器网络,实现采集数据及向网络发送数据的设备。它担负着数据采集、初步处理、加密和传输等多种功能。

感知识别型终端主要针对外部世界环境参数的采集,以二维码、RFID 传感器为主,实现对“物”的识别或者环境状态的感知。

应用型终端主要针对人的应用,提供键盘、鼠标、触摸屏和显示器等各种输入输出接口,例如计算机、平板电脑和智能手机等都属于此类终端。

物联网的感知识别型终端系统通常是嵌入式系统。嵌入式系统的安全对策可以分为安全电路层、硬件安全架构层、软件安全架构层和安全应用层等。

复习思考题

1. RFID 系统通常由哪几个部分组成?各部分的主要功能是什么?
2. RFID 系统的工作原理是什么?
3. 一套比较完美的 RFID 系统安全解决方案,应当具备哪些基本特征?
4. RFID 系统各部分的安全需求是什么?
5. 针对标签和读写器的攻击主要包括哪些手段?
6. 针对应用系统和后台数据库的攻击主要包括哪些手段?
7. RFID 系统的物理安全机制通常用于什么场合?
8. RFID 系统的物理安全机制主要包括哪些类别?
9. 什么是 RFID 系统的密码安全机制?
10. RFID 系统安全的密码机制包括哪些典型的安全认证协议?
11. 请画图并用文字说明 hash-lock(哈希锁)协议。
12. 请画图并用文字说明随机化 hash-lock(随机化哈希锁)协议。
13. 请画图并用文字说明 hash-chain(哈希链)协议。
14. 请画图并用文字说明 Hash 函数构造算法。
15. 请画图并用文字说明基于矩阵密钥的认证协议。
16. 请画图并用文字说明数字图书馆协议。
17. 什么是无线传感器网络?无线传感器网络由哪些部分组成?各部分的主要功能是什么?
18. 无线传感器网络的发展经历了哪几个阶段?
19. 无线传感器网络有哪些网络结构?
20. 无线传感器网络有哪些特点?
21. 无线传感器网络的安全威胁主要包括哪些手段?
22. 无线传感器网络中的信息安全需求主要包括哪些方面?

23. 请简要说明 S-MAC 协议的工作原理。
24. 请简要说明 SNEP 协议的工作原理。
25. 请简要说明 μTESLA 协议的工作原理。
26. 以数据为中心的路由协议包括哪些典型的协议？请简要说明每个典型的协议。
27. 层次式路由协议包括哪些典型的协议？请简要说明每个典型的协议。
28. 基于位置的路由协议包括哪些典型的协议？请简要说明每个典型的协议。
29. 无线传感器网络包括哪些典型的分布式密钥管理方案？
30. 无线传感器网络包括哪些典型的分簇式密钥管理方案？
31. 请说明物联网终端的 6 种不同分类的结果。
32. 请说明嵌入式系统的安全对策。

第5章 网络层安全技术

5.1 核心网安全技术

5.1.1 核心网安全概述

国际互联网或下一代网络(IPv6)是物联网网络层的核心载体。在物联网中,原来在国际互联网遇到的各种攻击问题依然存在,甚至更普遍,因此物联网需要有更完善的安全防护机制。不同的物联网终端设备的处理能力和网络能力差异较大,抵御网络攻击的防护能力也存在很大的差别,传统的国际互联网安全方案难以满足需求,并且也很难通过通用的安全方案解决所有安全问题,必须针对物联网的具体需求制定不同的安全方案。

核心网面临着原来的TCP/IP网络的所有安全问题,然而物联网又有其本身独有的特点。核心网安全问题的主要特点是海量,即存在海量的结点和海量的数据,因此对核心网的安全提出了更高的要求。核心网所面临的常见的安全问题主要包括以下几个方面:

1. DDoS攻击

由于核心网需要接收海量的、采用集群方式连接的物联网终端结点的信息,很容易导致网络拥塞,因此核心网极易受到分布式拒绝服务攻击(Distributed Denial of Service, DDoS),这也是物联网网络层遇到的最常见的攻击方式。因此,核心网必须解决的安全问题之一是如何对物联网脆弱结点受到的DDoS攻击进行防护。

2. 异构网络跨网认证

由于在物联网网络层存在不同架构的网络需要互相连通的问题,因此核心网也面临异构网络跨网认证等安全问题。在异构网络传输中,需要解决密钥和认证机制的一致性和兼容性等问题,而且还需要具有抵御DoS攻击、中间人攻击、异步攻击、合谋攻击等恶意攻击的能力。

3. 虚拟结点、虚拟路由信息攻击

由于物联网中的某些结点可以自由漫游,与邻近结点通信的关系在不断改变,结点的加入和脱离也许比较频繁,这样就很难为结点建立信任关系,从而导致物联网无基础结构,且

拓扑结构不断改变。因此入侵者可以通过虚拟结点、插入虚拟路由信息等方式对物联网发起攻击。

目前的物联网核心网主要是运营商的核心网络，核心网安全防护系统可以为物联网终端设备提供本地和网络应用的身份认证、网络过滤、访问控制、授权管理等安全服务。核心网的安全防护技术主要涉及网络加密技术、防火墙技术、隧道技术、网络虚拟化技术、黑客攻击与防范、计算机病毒防护、入侵检测技术、网络安全扫描技术等。

5.1.2　防火墙技术

1. 防火墙技术简介

所谓防火墙(Fire Wall)指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的边界上构造的保护屏障。

防火墙是一种保护计算机网络安全的技术性措施，它通过在网络边界上建立相应的网络通信监控系统来隔离内部和外部网络，以阻挡来自外部的网络入侵。

防火墙技术，最初是针对互联网的不安全因素所采取的一种防御保护措施。顾名思义，防火墙就是用来阻挡网络外部不安全因素影响的网络屏障，其目的就是防止外部网络用户未经授权的访问。它是一种计算机软件和硬件相互融合的技术，可使互联网与内部网(Intranet)之间建立起一个安全网关(Security Gateway)，从而保护内部网络免受非法用户的侵入。防火墙主要由服务访问政策、验证工具、包过滤和应用网关等 4 部分组成。防火墙是一个位于计算机和它所连接的网络之间的软件或硬件，流入或流出该计算机的所有网络通信数据都要经过此防火墙的过滤。

使用防火墙的好处有：保护脆弱的服务，控制对系统的访问，集中进行安全管理，增强保密性，记录和统计网络利用数据以及非法使用数据情况。防火墙的设计通常有两种基本设计策略：第一，允许任何服务除非被明确禁止；第二，禁止任何服务除非被明确允许。一般采用第二种策略。

2. 防火墙的工作原理

目前，防火墙技术已经发展成为一种成熟的保护计算机网络安全的技术。它是一种隔离控制技术，在某个机构的网络和不安全的网络(如 Internet)之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止重要信息从企业的网络上非法输出。

作为 Internet 网的安全性保护软件，防火墙已经得到广泛的应用。通常企业为了维护内部的信息系统安全，在企业网和 Internet 间设立防火墙软件。企业信息系统对于来自 Internet 的访问，采取有选择的接收方式。它可以允许或禁止某类具体的 IP 地址访问，也可以接收或拒绝 TCP/IP 上的某一类具体的应用。如果在某一台 IP 主机上有需要禁止的信息或危险的用户，则可以通过设置使用防火墙过滤掉从该主机发出的数据包。如果一个企业只是使用 Internet 的电子邮件和 WWW 服务器向外部提供信息，那么就可以在防火墙上设置只有这两类应用的数据包可以通过。这对于路由器来说，就要不仅分析 IP 层的信息，而且还要进一步了解 TCP 传输层甚至应用层的信息以进行取舍。防火墙一般安装在路由器上以保护一个子网，也可以安装在一台主机上，保护这台主机不受侵犯。

3. 防火墙的分类

从应用角度来分类，防火墙可以分为两大类，即网络防火墙和计算机防火墙。

网络防火墙如图 5-1 所示，网络防火墙是指在外部网络和企业内部网络之间设置网络防火墙。这种防火墙又称筛选路由器。网络防火墙检测进入信息的协议、目的地址、端口（网络层）及被传输的信息形式（应用层）等，过滤并清除不符合规定的外来信息。网络防火墙也对用户内部网络向外部网络发出的信息进行检测。

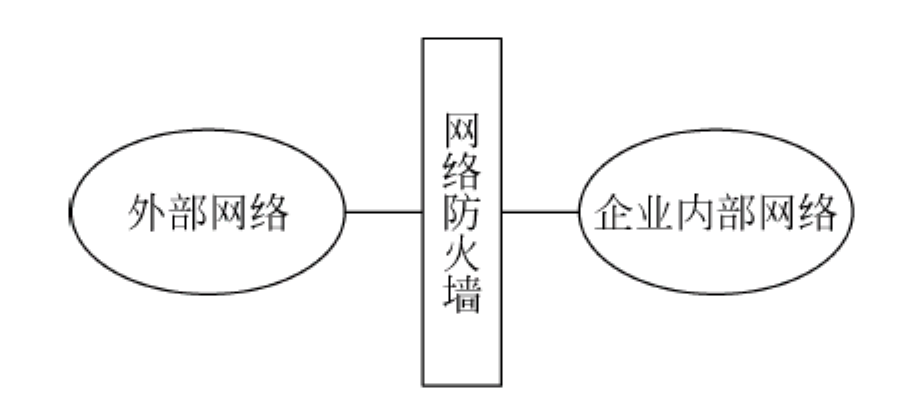


图 5-1　网络防火墙

计算机防火墙如图 5-2 所示。计算机防火墙是指在外部网络和用户计算机之间设置防火墙。计算机防火墙也可以是用户计算机的一部分。计算机防火墙检测接口规程、传输协议、目的地址及/或被传输的信息结构等，将不符合规定的进入信息剔除。计算机防火墙对用户计算机输出的信息进行检查，并加上相应协议层的标志，用以将信息传送到接收用户计算机（或网络）中去。

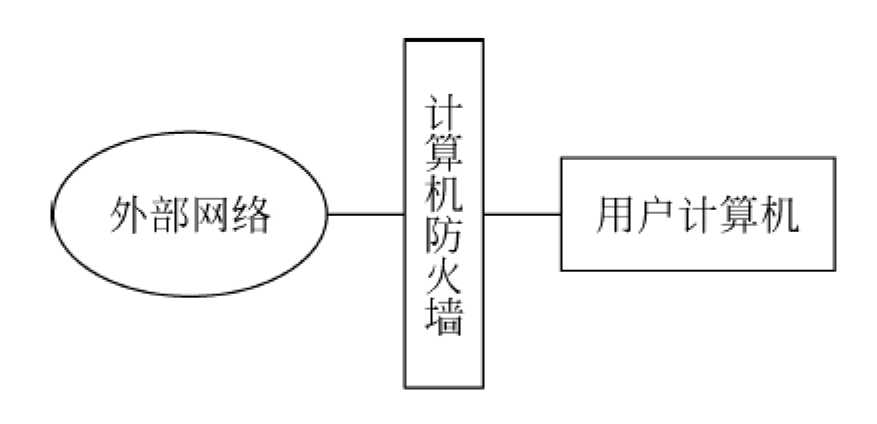


图 5-2　计算机防火墙

从工作原理来分类，防火墙可以分为四大类：网络级防火墙（也称为包过滤型防火墙）、应用级网关、电路级网关和规则检查防火墙。它们之间各有所长，具体使用哪一种或是否混合使用，则要由企业的实际需求来确定。

1）网络级防火墙

网络级防火墙一般是基于源地址和目的地址、应用、协议以及每个 IP 包的端口来作出通过与否的判断。一个路由器便是一个“传统”的网络级防火墙，大多数的路由器都能通过检查这些信息来决定是否将所收到的包转发，但它不能判断出一个 IP 包来自何方，去向何处。防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。

2）应用级网关

应用级网关能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客

户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议,能够做复杂一些的访问控制,并做精细的注册和稽核。它针对特别的网络应用服务协议即数据过滤协议,并且能够对数据包分析并形成相关的报告。应用网关对某些易于登录和控制所有输出输入的通信的环境给予严格的控制,以防有价值的程序和数据被窃取。在实际工作中,应用网关一般由专用工作站系统来完成。但每一种协议需要相应的代理软件,使用时工作量大,效率不如网络级防火墙。应用级网关有较好的访问控制,是目前最安全的防火墙技术,但实现困难,而且有的应用级网关缺乏“透明度”。在实际使用中,用户在受信任的网络上通过防火墙访问 Internet 时,经常会发现存在延迟并且必须进行多次登录(Login)才能访问 Internet 或 Intranet。

3) 电路级网关

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息,以便来决定该会话(Session)是否合法,电路级网关是在 OSI 模型中会话层上来过滤数据包,这样比包过滤防火墙要高二层。电路级网关还提供一个重要的安全功能:代理服务器(Proxy Server)。代理服务器是设置在 Internet 防火墙网关的专用应用级代码。这种代理服务准许网管员允许或拒绝特定的应用程序或一个应用的特定功能。包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许特定的数据包通过,一旦判断条件满足,防火墙内部网络的结构和运行状态便“暴露”在外来用户面前,这就引入了代理服务的概念,即防火墙内外计算机系统应用层的“链接”由两个终止于代理服务的“链接”来实现,这就成功地实现了防火墙内外计算机系统的隔离。同时,代理服务还可用于实施较强的数据流监控、过滤、记录和报告等功能。代理服务技术主要通过专用计算机硬件(如工作站)来承担。

4) 规则检查防火墙

规则检查防火墙综合了包过滤防火墙、电路级网关和应用级网关的优点。它与包过滤防火墙一样,规则检查防火墙能够在 OSI 网络层上通过 IP 地址和端口号,过滤进出的数据包。它也如同电路级网关一样,能够检查 SYN 和 ACK 标记和序列数字是否逻辑有序。当然,它也如同应用级网关一样,可以在 OSI 应用层上检查数据包的内容,查看这些内容是否能符合企业网络的安全规则。规则检查防火墙虽然集成前三者的特点,但是不同于一个应用级网关的是,它并不打破客户机/服务器模式来分析应用层的数据,它允许受信任的客户机和不受信任的主机建立直接连接。规则检查防火墙不依靠与应用层有关的代理,而是依靠某种算法来识别进出的应用层数据,这些算法通过已知合法数据包的模式来比较进出数据包,这样从理论上就能比应用级代理在过滤数据包上更有效。

4. 防火墙的功能

防火墙对流经它的网络通信进行扫描,这样能够过滤掉一些攻击,以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信,封锁特洛伊木马。最后,它可以禁止来自特殊站点的访问,从而防止来自不明入侵者的所有通信。

1) 网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环

境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议访问受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2）强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如密码、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密的密码系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙上。

3）监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4）防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的服务，如 Finger，DNS 等服务。Finger 服务显示主机的所有用户的注册名和真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙同样可以阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN（虚拟专用网）。

5）数据包过滤

网络上的数据都是以包为单位进行传输的，每一个数据包中都会包含一些特定的信息，如数据的源地址、目标地址、源端口号和目标端口号等。防火墙通过读取数据包中的地址信息来判断这些包是否来自可信任的网络，并与预先设定的访问控制规则进行比较，进而确定是否需对数据包进行处理和操作。数据包过滤可以防止外部不合法用户对内部网络的访问，但由于不能检测数据包的具体内容，所以不能识别具有非法内容的数据包，无法实施对应用层协议的安全处理。

6）网络 IP 地址转换

网络 IP 地址转换是一种将私有 IP 地址转化为公网 IP 地址的技术，它被广泛应用于各种类型的网络和互联网的接入中。网络 IP 地址转换一方面可隐藏内部网络的真实 IP 地址，使内部网络免受黑客的直接攻击；另一方面由于内部网络使用了私有 IP 地址，从而有效解决了公网 IP 地址不足的问题。

7）虚拟专用网络

虚拟专用网络将分布在不同地域上的局域网或计算机通过加密通信，虚拟出专用的传输通道，从而将它们从逻辑上连成一个整体，不仅省去了建设专用通信线路的费用，还有效地保证了网络通信的安全。

8）日志记录与事件通知

进出网络的数据都必须经过防火墙，防火墙通过日志对其进行记录，能提供网络使用的详细统计信息。当发生可疑事件时，防火墙能根据安全机制进行报警和通知，提供网络是否受到威胁的信息。

5. 防火墙技术的应用

防火墙技术对物联网具有很好的保护作用。入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机。网络管理员可以将防火墙配置成许多不同保护级别。高级别的保护可能会禁止一些服务，如视频流等，但这是提高内部网络安全性的有效措施。

在应用防火墙技术时，还应当注意以下两个方面：

(1) 防火墙是不能防御病毒的，尽管有不少的防火墙产品声称自己具有防病毒功能。

(2) 防火墙技术的另外一个缺点是在防火墙之间的数据难以更新，如果数据更新需要延迟太长的时间，将无法响应实时服务请求。此外，防火墙采用滤波技术，滤波通常会使网络的传输性能降低50%以上，如果为了改善网络性能而购置高速路由器，又会大大增加网络设备的经费。

总之，防火墙技术是物联网安全的一种可行技术，它可以把公共数据和服务置于防火墙外，使其对防火墙内部资源的访问受到限制。作为一种网络安全技术，防火墙具有简单实用的特点，并且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求。

5.1.3 网络虚拟化技术

1. 网络虚拟化技术概述

网络虚拟化一般指虚拟专用网络(Virtual Private Network，VPN)。VPN 对网络连接的概念进行了抽象，允许用户远程地访问企业或组织的内部网络，就像物理上连接到该网络一样。网络虚拟化可以帮助保护 IT 环境，防止来自 Internet 的威胁，同时使用户能够快速地、安全地访问企业内部的应用程序和数据。

虚拟专用网络是通过公用网络(通常是国际互联网)建立的临时的、安全的特殊网络，是一条穿过公用网络的、安全的、稳定的加密隧道。使用这条隧道可以对数据进行加密，以达到安全使用互联网的目的。

虚拟专用网络可以实现不同网络的组件和资源之间的相互连接。虚拟专用网络能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。虚拟专用网络的结构如图 5-3 所示。

在企业的内部网络中，考虑到一些部门可能存储有重要数据，为确保数据的安全性，传统的方式只能是把这些部门同整个企业网络断开形成孤立的小网络。这样做虽然保护了部门的重要信息，但是由于物理上的中断，使其他部门的用户无法访问，造成通信上的困难。

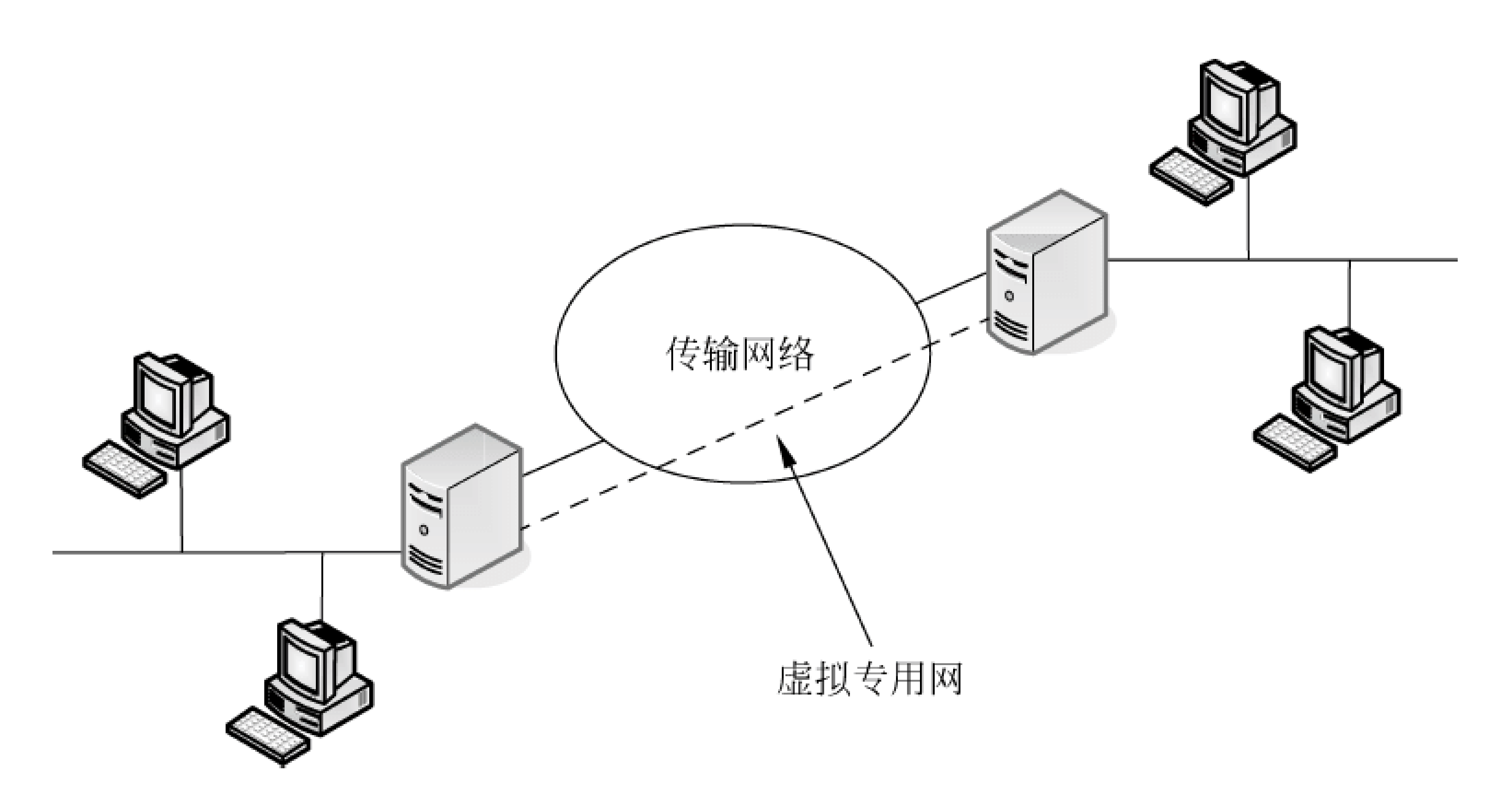


图 5-3 虚拟专用网络的结构

采用 VPN 方案,通过使用一台 VPN 服务器既能够实现与整个企业网络的连接,又可以保证保密数据的安全性。路由器虽然也能够实现网络之间的互联,但是并不能对流向敏感网络的数据进行限制。企业网络管理人员通过使用 VPN 服务器,指定只有符合特定身份要求的用户才能连接 VPN 服务器获得访问敏感信息的权利。此外,可以对所有 VPN 数据进行加密,从而确保数据的安全性。没有访问权利的用户无法看到部门的局域网络。

虚拟专用网络允许远程通信方,销售人员或企业分支机构使用 Internet 等公共互联网络的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。虚拟专用网络对用户端透明,用户好像使用一条专用线路在客户计算机和企业服务器之间建立点对点连接,进行数据的传输。

虚拟专用网络技术同样支持企业通过 Internet 等公共互联网络与分支机构或其他公司建立连接,进行安全的通信。这种跨越 Internet 建立的 VPN 连接逻辑上等同于两地之间使用广域网建立的连接。

虽然 VPN 通信建立在公共互联网络的基础上,但是用户在使用 VPN 时感觉如同在使用专用网络进行通信,所以得名虚拟专用网络。

使用 VPN 技术可以解决在当今远程通信量日益增大,企业全球运作广泛分布的情况下,员工需要访问中央资源,企业相互之间必须进行及时和有效的通信的问题。

虚拟专用网络支持以安全的方式通过公共互联网络远程访问企业资源。

在选择 VPN 技术时,一定要考虑管理上的要求。一些大型网络都需要把每个用户的目录信息存放在一台中央数据存储设备中(目录服务)便于管理人员和应用程序对信息进行添加,修改和查询。每一台接入或隧道服务器都应当能够维护自己的内部数据库,存储每一个用户的账户信息,包括用户名、密码以及拨号接入的属性等。但是,这种由多台服务器维护多个用户账户的做法,很难实现及时的同步更新,这给管理带来很大的困难。因此,大多数的网络管理员采用在目录服务器、主域控制器或 RADIUS 服务器上,建立一个主账号数据库的方法,来进行统一的、有效的管理。

2. 虚拟专用网络的连接方式

通常可以采用以下两种方式来实现远程企业内部网络的连接。

1）使用专线连接分支机构和企业局域网

专线方式不需要使用价格昂贵的长距离专用线路，分支机构和企业端的路由器可以使用各自本地的专用线路，通过本地的 ISP 连通 Internet。通过 VPN 软件与本地 ISP 建立连接的方式，在 Internet 与分支机构和企业端的路由器之间建立一个虚拟专用网络。

2）使用拨打本地 ISP 号码的方式连接分支机构和企业内部网

区别于传统的连接分支机构路由器的拨打长途电话的方式，分支机构端的路由器可以通过拨号方式连接本地 ISP。VPN 软件使用与本地 ISP 建立起的连接，在分支机构和企业端路由器之间创建一个跨越 Internet 的虚拟专用网络。

值得注意的是，在上述两种方式中，是通过使用本地设备在分支机构和企业部门与 Internet 之间建立连接。无论是在客户端还是服务器端，都是通过拨打本地接入电话建立连接，因此 VPN 可以大大节省连接的费用。建议将 VPN 服务器的企业端路由器以专线方式连接本地 ISP。VPN 服务器必须一天 24 小时对 VPN 数据流进行监听。

3. VPN 系统的安全需求

一般来说，企业在选用一种远程网络互联方案时，都希望能够对访问企业资源和信息的要求加以控制，所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接，不同分支机构之间的资源共享；又能够确保企业数据在公共互联网络或企业内部网络上传输时安全性不受破坏。因此，一个成熟的 VPN 系统应当能够同时满足以下几个方面的安全需求：

1）身份认证

VPN 系统必须能够认证用户的身份，并且严格控制只有授权用户才能访问 VPN。此外，方案还必须能够提供审计和计费功能，能够追踪到什么人、在什么时候访问了 VPN。

2）地址管理

VPN 系统必须能够为用户分配专用网络上的地址并确保地址的安全性。

3）数据加密

对通过公共互联网络传递的数据必须经过加密，确保网络其他未授权的用户无法读取该信息。

4）密钥管理

VPN 系统必须能够生成并更新客户端和服务器的加密密钥。

5）多协议支持

VPN 系统必须支持公共互联网络上普遍使用的基本协议，包括 IP、IPX 协议等。以点对点隧道协议（PPTP）或第 2 层隧道协议（L2TP）为基础的 VPN 方案，既能够满足以上所有的基本要求，又能够充分利用遍及世界各地的 Internet 互联网络的优势。其他方案，包括安全 IP 协议（IPSec），虽然不能满足上述全部要求，但是仍然适用于在特定的环境。以下将主要集中讨论有关 VPN 的概念、协议和部件（Component）。

4. 隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或

包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据将被解包并转发到最终目的地。注意隧道技术是指包括数据封装，传输和解包在内的全过程。

隧道所使用的传输网络可以是任何类型的公共互联网络，本节主要以目前广泛使用Internet为例进行说明。此外，在企业网络同样可以创建隧道。隧道技术在经过一段时间的研究、发展和完善之后，已经逐渐成熟。常用的隧道技术主要包括：

1）IP 网络上的 SNA 隧道技术

当系统网络结构（System Network Architecture，SNA）的数据流通过企业 IP 网络传送时，SNA 数据帧将被封装在 UDP 和 IP 协议包头中。

2）IP 网络上的 Novell NetWare IPX 隧道技术

当一个 IPX 数据包被发送到 NetWare 服务器或 IPX 路由器时，服务器或路由器用 UDP 和 IP 包头封装 IPX 数据包后通过 IP 网络发送。另一端的 IP-TO-IPX 路由器在去除 UDP 和 IP 包头之后，把数据包转发到 IPX 目的地。

3）点对点隧道协议（PPTP）

PPTP 协议允许对 IP，IPX 或 NetBEUI 数据流进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共互联网络发送。

4）第 2 层隧道协议（L2TP）

L2TP 协议允许对 IP，IPX 或 NetBEUI 数据流进行加密，然后通过支持点对点数据报传递的任意网络发送，如 IP、X. 25、帧中继或 ATM。

5）安全 IP（IPSec）隧道模式

IPSec 隧道模式允许对 IP 负载数据进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共 IP 互联网络如 Internet 发送。

5. 隧道协议分析

为了创建隧道，隧道的客户机和服务器双方都必须遵守相同的隧道协议。

隧道技术可以分别以第 2 层或第 3 层隧道协议为基础。分层按照开放系统互联（OSI）的参考模型划分。第 2 层隧道协议对应 OSI 模型中的数据链路层，使用帧作为数据交换单位。PPTP，L2TP 和 L2F（第 2 层转发）都属于第 2 层隧道协议，都是将数据封装在点对点协议（PPP）帧中通过互联网络发送。第 3 层隧道协议对应 OSI 模型中的网络层，使用包作为数据交换单位。IP over IP 以及 IPSec 隧道模式都属于第 3 层隧道协议，都是将 IP 包封装在附加的 IP 包头中通过 IP 网络传送的。

对于像 PPTP 和 L2TP 这样的第 2 层隧道协议，创建隧道的过程类似于在双方之间建立会话；隧道的两个端点必须同意创建隧道并协商隧道各种配置变量，如地址分配，加密或压缩等参数。绝大多数情况下，通过隧道传输的数据都使用基于数据报的协议发送。隧道维护协议被用来作为管理隧道的机制。

第 3 层隧道技术通常假定所有配置问题已经通过手工过程完成。这些协议不对隧道进行维护。与第 3 层隧道协议不同，第 2 层隧道协议（PPTP 和 L2TP）必须包括对隧道的创

建、维护和终止。

隧道客户端和服务器使用隧道数据传输协议传输数据。隧道一旦建立，数据就可以通过隧道传输。当隧道客户端向服务器端发送数据时，客户端首先给负载数据加上一个隧道数据传送协议包头，然后把封装好的数据通过互联网络发送，并由互联网络将数据转发到隧道的服务器端。隧道的服务器端收到数据包之后，会删除隧道数据传输协议包头，然后将负载数据转发到目标网络。

1）第 2 层隧道协议的特点

第 2 层隧道协议（PPTP 和 L2TP）以完善的 PPP 协议为基础，它继承了 PPP 协议的特性。

（1）用户验证。

第 2 层隧道协议继承了 PPP 协议的用户验证方式。许多第 3 层隧道技术都假定在创建隧道之前，隧道的两个端点相互之间已经了解或已经经过验证。一个例外情况是 IPSec 协议的 ISAKMP 协商提供了隧道端点之间进行的相互验证。

（2）令牌卡（Token Card）支持。

通过使用扩展验证协议（EAP），第 2 层隧道协议能够支持多种验证方法，包括一次性密码（one-time password），加密计算器（cryptographic calculator）和智能卡等。第 3 层隧道协议也支持使用类似的方法，例如，IPSec 协议通过 ISAKMP/Oakley 协商确定公共密钥证书验证。

（3）动态地址分配。

第 2 层隧道协议支持在网络控制协议（NCP）协商机制的基础上动态分配客户地址。第 3 层隧道协议通常假定隧道建立之前已经进行了地址分配。目前 IPSec 隧道模式下的地址分配方案仍在开发之中。

（4）数据压缩。

第 2 层隧道协议支持基于 PPP 的数据压缩方式。例如，微软的 PPTP 和 L2TP 方案使用微软点对点加密协议（MPPE）。IETP 正在开发应用于第 3 层隧道协议的类似数据压缩机制。

（5）数据加密。

第 2 层隧道协议支持基于 PPP 的数据加密机制。微软的 PPTP 方案支持在 RSA/RC4 算法的基础上选择使用 MPPE。第 3 层隧道协议可以使用类似方法，例如，IPSec 通过 ISAKMP/Oakley 协商确定几种可选的数据加密方法。微软的 L2TP 协议使用 IPSec 加密保障隧道客户端和服务器之间数据流的安全。

（6）密钥管理。

作为第 2 层协议的 MPPE 依靠验证用户时生成的密钥，定期对其更新。IPSec 在 ISAKMP 交换过程中公开协商公用密钥，同样对其进行定期更新。

（7）多协议支持。

第 2 层隧道协议支持多种负载数据协议，从而使隧道客户能够访问使用 IP，IPX，或 NetBEUI 等多种协议企业网络。相反，第 3 层隧道协议，如 IPSec 隧道模式只能支持使用 IP 协议的目标网络。

一旦完成了协商，PPP 就开始在连接对等双方之间转发数据。每个被传送的数据报都

被封装在 PPP 包头内，该包头将会在到达接收方之后被去除。如果在阶段 1 选择使用数据压缩并且在阶段 4 完成了协商，数据将会在被传送之间进行压缩。类似地，如果已经选择使用数据加密并完成了协商，数据(或被压缩数据)将会在传送之前进行加密。

2）点对点隧道协议

点对点隧道协议(PPTP)是一个第 2 层的协议，将 PPP 数据帧封装在 IP 数据报内通过 IP 网络，如 Internet 传送。PPTP 还可用于专用局域网络之间的连接。RFC 草案“点对点隧道协议”对 PPTP 协议进行了说明和介绍。该草案由 PPTP 论坛的成员公司，包括微软、Ascend、3Com 和 ECI 等公司在 1996 年 6 月提交至 IETF。

PPTP 使用一个 TCP 连接对隧道进行维护，使用通用路由封装(GRE)技术把数据封装成 PPP 数据帧通过隧道传送。可以对封装 PPP 帧中的负载数据进行加密或压缩。

3）第 2 层转发协议

第 2 层转发协议(L2F)是 Cisco 公司提出的一种隧道技术。作为一种传输协议，L2F 支持拨号接入服务器将拨号数据流封装在 PPP 帧内，并通过广域网链路传送到 L2F 服务器(路由器)。L2F 服务器把数据包解压后，重新转发到网络。与 PPTP 和 L2TP 不同，L2F 没有确定的客户端。应当注意，L2F 隧道技术仅仅在强制隧道中有效。

4）第 2 层隧道协议(L2TP)

第 2 层隧道协议综合了 PPTP 和 L2F 协议的优点。设计者希望 L2TP 能够综合 PPTP 和 L2F 的优势。L2TP 是一种网络层协议，支持封装的 PPP 帧在 IP，X. 25，帧中继或 ATM 等的网络上进行传送。当使用 IP 作为 L2TP 的数据报传输协议时，可以使用 L2TP 作为 Internet 网络上的隧道协议。L2TP 还可以直接在各种 WAN 媒介上使用而不需要使用 IP 传输层。

IP 网上的 L2TP 使用 UDP 和一系列的 L2TP 消息对隧道进行维护。L2TP 同样使用 UDP 将 L2TP 协议封装的 PPP 帧通过隧道发送。可以对封装 PPP 帧中的负载数据进行加密或压缩。

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。尽管这两个协议非常相似，但是两者仍然存在以下区别：

(1) PPTP 要求互联网络为 IP 网络。

L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP(使用 UDP)、帧中继永久虚拟电路(PVC)、X. 25 虚拟电路(VC)或 ATM VC 网络上使用。

(2) PPTP 只能在两端点间建立单一隧道。

L2TP 支持在两端点间使用多隧道。使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。

(3) L2TP 可以提供包头压缩。

当压缩包头时，系统开销(overhead)占用 4 个字节，而 PPTP 协议下要占用 6 个字节。

(4) 隧道验证。

L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第 2 层协议上验证隧道。

6. IPSec 隧道技术

IPSec 协议是一种工作在网络层的网络协议，支持 IP 网络上数据的安全传输。除了对 IP 数据流的加密机制进行了规定之外，IPSec 协议还定义了 IP over IP 隧道模式的数据包格式，一般被称作 IPSec 隧道模式。一个 IPSec 隧道由一个隧道客户和隧道服务器组成，两端都配置使用 IPSec 隧道技术，采用协商加密机制。

为实现在专用或公共 IP 网络上的安全传输，IPSec 隧道模式使用的安全方式封装和加密整个 IP 包。然后对加密的负载再次封装在明文 IP 包头内通过网络发送到隧道服务器端。隧道服务器对收到的数据报进行处理，在去除明文 IP 包头，对内容进行解密之后，获得最初的负载 IP 包。负载 IP 包在经过正常处理之后被路由到位于目标网络的目的地。

IPSec 隧道模式具有以下特点：

(1) 只能支持 IP 数据流。

(2) 工作在 IP 栈(IP Stack)的底层，因此，应用程序和高层协议可以继承 IPSec 的行为。

(3) 由一个安全策略(一整套过滤机制)进行控制。安全策略按照优先级的先后顺序创建可供使用的加密和隧道机制以及验证方式。当需要建立通信时，双方机器执行相互验证，然后协商使用何种加密方式。此后的所有数据流都将使用双方协商的加密机制进行加密，然后封装在隧道包头内。

IPSec 隧道技术是一种由国际互联网工程任务组(Internet Engineering Task Force, IETF)定义的、端到端的、确保基于 IP 通信的数据安全性的机制。IPSec 支持对数据加密，同时确保数据的完整性。按照 IETF 的规定，不采用数据加密时，IPSec 使用验证包头(AH)提供验证来源验证(Source Authentication)，确保数据的完整性；采用数据加密时，IPSec 使用封装安全负载(ESP)与加密一道提供来源验证，确保数据完整性。IPSec 协议下，只有发送方和接受方知道加密密钥。如果验证数据有效，接收方就可以知道数据来自发送方，并且在传输过程中没有受到破坏。

我们可以把 IPSec 协议理解为位于 TCP/IP 协议栈的下层协议。该层由每台机器上的安全策略和发送、接收方协商的安全关联(Security Association)进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的 IP 地址、协议和端口号满足过滤机制，那么这个数据包必须遵守关联的安全行为。

第一个满足过滤机制的数据包将会引发发送方和接收方对安全关联进行协商。ISAKMP/OAKLEY 是这种协商采用的标准协议。在一个 ISAKMP/OAKLEY 交换过程中，两台机器对验证和数据安全方式达成一致，进行相互验证，然后生成一个用于随后的数据加密的共享密钥。

通过一个位于 IP 包头和传输包头之间的验证包头可以提供 IP 负载数据的完整性和数据验证。验证包头包括验证数据和一个序列号，共同用来验证发送方身份，确保数据在传输过程中没有被改动，防止受到第三方的攻击。IPSec 验证包头不提供数据加密；信息将以明文方式发送。

为了保证数据的保密性并防止数据被第 3 方窃取，封装安全负载(ESP)提供了一种对 IP 负载进行加密的机制。另外，ESP 还可以提供数据验证和数据完整性服务；因此在

IPSec 数据包中，可以用 ESP 包头替代 AH 包头。

5.1.4 黑客攻击与防范

1. 黑客的基本概念

黑客一般是指网络的非法入侵者，他们往往是优秀的程序员，具有计算机网络和物联网的软件及硬件的高级知识，并有能力通过一些特殊的方法剖析和攻击网络。黑客以破坏网络系统为目的，往往采用某些不正当的手段找出网络的漏洞，并利用网络漏洞破坏计算机网络或物联网，从而危害网络的安全。

2. 黑客常用的攻击方法

1）窃取密码

窃取密码是最常见的攻击方法之一。一般来说，黑客窃取密码会使用以下三种方法：

（1）通过网络监听非法获得用户的密码，这类方法虽然有一定的局限性，但是危害性极大，监听者往往能够获得其所在网段的所有用户账号和密码，对局域网安全威胁巨大；

（2）在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户密码，这种方法不受网段限制，但黑客要有足够的耐心和时间；

（3）在首先获得一个服务器上的用户密码文件（Shadow 文件）后，再用暴力破解程序破解用户密码，应用这种方法的前提条件是黑客要先获得密码的 Shadow 文件。

在黑客窃取密码的这三种方法中，第三种方法的危害最大，因为它不需要像第二种方法那样，一遍又一遍地尝试登录服务器，而是在本地将加密后的密码与 Shadow 文件中的密码相比较，就可以非常容易地破获用户的密码，尤其对那些安全意识薄弱的用户。

某些用户设置的密码安全系数极低，例如某个用户的账号为 zys，他将密码简单地设置为 zys123、123456 等，因此，黑客仅仅需要花短短的几分钟，甚至几十秒内就可以猜出密码。

2）特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它经常被伪装成工具软件或者游戏软件，诱使用户运行从网上下载的带有特洛伊木马程序的软件，或者打开带有特洛伊木马程序的电子邮件附件，一旦用户运行了特洛伊木马程序之后，它们就会像古代特洛伊人在敌人城外留下的藏匿了士兵的木马一样隐藏在用户的电脑中，并在用户的计算机系统中隐藏一个可以在 Windows 操作系统启动时悄悄执行的程序。当用户连接到互联网上时，这个程序就会通知黑客，并报告用户的 IP 地址以及预先设定的端口。黑客在收到这些信息后，利用这个潜伏在其中的木马程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户的计算机的目的。

3）www 欺骗技术

在互联网上，用户可以利用 IE 等网页浏览器访问各种各样的网站，如浏览新闻、查询产品价格、进行证券交易、电子商务等。

然而，许多用户也许不会想到，这些常用的、简单的上网操作，存在着严重的安全隐患。例如，访问的网页已经被黑客篡改过，网页上的信息是虚假的。黑客很可能将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览这些网页的时候，实际上是向黑客

服务器发送信息，那么黑客就可以轻易窃取用户的机密信息，如登录的账号和密码等，从而达到欺骗的目的。

4）电子邮件攻击

电子邮件攻击主要表现为两种方式：第一种方式是电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重的可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；第二种方式是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改密码（密码可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序。某些单位的网络管理员有定期给用户免费发送防火墙升级程序的责任，这为黑客成功地利用该方法提供了可乘之机。

5）通过一个结点来攻击其他结点

黑客在攻破一台主机后，往往以此主机作为根据地，继续攻击其他主机，从而隐蔽其入侵路径，避免留下蛛丝马迹。黑客往往使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。这类攻击很狡猾，但由于这种技术很难掌握，如 IP 欺骗，因此较少被黑客使用。

6）网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，就可以轻而易举地截取包括密码和账号在内的信息资料。虽然网络监听获得的用户账号和密码具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及密码。

7）寻找系统漏洞

许多操作系统都有这样那样的安全漏洞（Bug），其中某些是操作系统或应用软件本身具有的，如 Windows 中的共享目录密码验证漏洞和 IE 浏览网漏洞等，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，除非你将网线拔掉；还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出，将未加 Shadow 的用户密码文件以明码方式存放在某一目录下，这都会给黑客带来可乘之机，应及时加以修正。

8）利用账号进行攻击

有些黑客会利用操作系统的默认账户和密码进行攻击，例如许多 UNIX 主机都有 FTP 和 Guest 等默认账户（其密码和账户名同名），有的甚至没有密码。黑客用 UNIX 操作系统提供的命令如 Finger 和 Ruser 等收集信息，不断提高自己的攻击能力。针对这类攻击，只要系统管理员将系统提供的默认账户关掉或提醒无密码用户增加密码，一般都能克服。

9）获取特权

利用各种特洛伊木马程序、后门程序和黑客自己编写的导致缓冲区溢出的程序进行攻击，前者可使黑客非法获得对用户机器的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段，一旦奏效，危害性极大。

3. 黑客常用的攻击步骤

黑客的攻击手段变幻莫测，但纵观其整个攻击过程，还是有一定规律可循的，通常可以分为攻击前奏、实施攻击、巩固控制、继续深入等四个步骤。

1）攻击前奏

黑客锁定目标、了解目标的网络结构，收集各种目标系统的信息等。网络上有许多主机，黑客首先要寻找他要攻击的网站，锁定目标的 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。

锁定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关、路由器，哪里有防火墙，哪些主机与要攻击的目标主机关系密切等，最简单的就是用 tracert 命令追踪路由，也可以发一些数据包看其是否能通过，来猜测其防火墙过滤规则的设定等。当然经验丰富的黑客在探测目标主机信息的时候，往往会利用其他计算机来间接地探测，从而隐藏他们真实的 IP 地址。

在收集到目标的第一批网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。首先黑客要知道目标主机采用的是什么操作系统什么版本，如果目标开放 telnet 服务，那只要 telnet xx. xx. xx. xx.（目标主机），就会显示 digitalunlx（xx. xx. xx. xx）（ttypl）login：这样的系统信息。收集系统信息当然少不了安全扫描器，黑客往往会利用安全扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞，应用软件漏洞，弱密码用户等。

接着黑客还会检查其开放端口进行服务分析，看是否有能被利用的服务。因特网上的主机大部分都开放 www、mail、ftp、telnet 等日常网络服务，通常情况下 telnet 服务的端口是 23 等，www 服务的端口是 80，ftp 服务的端口是 23。利用信息服务，像 snmp 服务、traceroute 程序、whois 服务可用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节，traceroute 程序能够用该程序获得到达目标主机所要经过的网络数和路由器数，whois 协议服务能提供所有有关的 dns 域和相关的管理参数，finger 协议可以用 finger 服务来获取一个指定主机上的所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等等）。所以如果没有特殊的需要，管理员应该关闭这些服务。

2）实施攻击

当黑客收集到了足够的目标主机的信息，对系统的安全弱点有一定的了解后就会发起攻击。当然，黑客们会根据不同的网络结构、不同的系统情况而采用不同的攻击手段。黑客攻击的最终目的是能够控制目标系统，窃取其中的机密文件等。但是，黑客的攻击未必能够得逞，达到控制目标主机的目的。因此，有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作，甚至瘫痪。

3）巩固控制

黑客利用种种手段进入目标主机系统并获得控制权之后，未必会立即进行破坏活动，删除数据、涂改网页等，这是黑客新手的行为。一般来说，入侵成功后，黑客为了能长期地保留和巩固他对系统的控制权，不被管理员发现，他都会做两件事：清除记录和留下后门。日志往往会记录上一些黑客攻击的蛛丝马迹，黑客当然不会留下这些“犯罪证据”，他会把它删了

或用假日志覆盖它,以便日后不被觉察地再次进入系统。黑客还会更改某些系统设置,在系统中置入特洛伊木马或其他一些远程操纵程序。

4) 继续深入

使用清除日志、删除复制的文件等手段来隐藏自己的踪迹之后,攻击者通常就会采取下一步的行动,窃取主机上的各种敏感信息:如客户名单和通信录、财务报表、信用卡账号和密码、用户的相片等,也可能是什么都不动,只是把用户的系统作为他存放黑客程序或资料的仓库,黑客也可能会利用这台已经攻陷的主机去继续他下一步的攻击,如:继续入侵内部网络,或者利用这台主机发动 DoS 攻击使网络瘫痪。

网络世界瞬息万变,黑客们各有不同,他们的攻击流程也不会完全相同,以上提到的攻击步骤是概括而言的,是绝大部分黑客一般情况下采用的攻击步骤。

4. 防范黑客攻击的对策

黑客对服务器进行扫描是轻而易举的,一旦让黑客找到了服务器存在的漏洞,则其后果是非常严重的。因此,作为网络管理员应该采取必要的技术手段,防范黑客对服务器进行攻击。以下介绍针对黑客各种不同的攻击行为,网络管理员应当采取的防御对策。

1) 屏蔽可疑的 IP 地址

这种方法见效最快,一旦网络管理员发现了可疑的 IP 地址,可以通过防火墙屏蔽相应的 IP 地址,这样黑客就无法再连接到服务器上了。但是这种方法有很多缺点,例如很多黑客都使用的动态 IP,也就是说他们的 IP 地址会变化,一个地址被屏蔽,只要更换其他 IP 仍然可以进攻服务器,而且某些黑客有可能伪造 IP 地址,使屏蔽 IP 地址无法奏效。

2) 过滤信息包

网络管理员可以通过编写防火墙规则,让系统知道什么样的信息包允许进入、什么样的信息包应该放弃,如此一来,当黑客发送有攻击性信息包经过防火墙时,信息包就会被丢弃掉,从而防止了黑客的攻击。但是这种做法仍然有不足之处,例如黑客可以修改攻击性代码的方式,使防火墙分辨不出信息包的真假;或者黑客干脆无休止的、大量地发送信息包,直到服务器不堪重负而造成系统崩溃。

3) 修改系统协议

对于漏洞扫描,网络管理员可以修改服务器的相应协议来进行防御。例如,漏洞扫描是根据对文件扫描的返回值来判断文件是否存在的。在正常情况下,如果返回值是 200,则表示服务器存在这个文件;如果返回值是 404,则表明服务器上没有这个的文件。假如网络管理员修改了返回文件返回值,那么黑客就无法通过漏洞扫描检测文件是否存在了。

4) 修补安全漏洞

任何一个版本的操作系统发布之后,在短时间内都不会受到攻击,一旦其中的问题暴露出来,黑客就会蜂拥而至。因此管理员在维护系统的时候,可以经常浏览著名的安全站点,找到系统的新版本或者补丁程序进行安装,这样就可以保证系统中的安全漏洞在没有被黑客发现之前,就已经修补上了,从而保证了服务器的安全。

5) 及时备份重要数据

亡羊补牢,犹未为晚。如果及时做好了数据备份,即便系统遭到黑客进攻,也可以在短时间内修复,挽回不必要的经济损失。许多大型网站,都会在每天晚上对系统数据库进行备

份，在次日清晨，无论系统是否受到攻击，都会重新恢复数据，保证每天系统中的数据库都不会出现损坏。备份的数据库文件最好存放到其他电脑的硬盘或者磁带上，这样黑客进入服务器之后，破坏的数据只是一部分，因为无法找到数据的备份，对于服务器的损失也不会太严重。

一旦受到黑客攻击，网络管理员不要仅仅设法恢复损坏的数据，还要及时分析黑客的来源和攻击方法，尽快修补被黑客利用的漏洞，然后检查系统中是否被黑客安装了木马、蠕虫或者被黑客开放了的某些管理员账号，尽量将黑客留下的各种蛛丝马迹和后门分析、清除干净，防止黑客的下一次攻击。

6）使用加密机制传输数据

对于个人信用卡、密码等重要数据，在客户端与服务器之间的传送，应该事先经过加密处理再进行发送，这样做的目的是防止黑客监听、截获。对于现在网络上流行的各种加密机制，都已经出现了不同的破解方法，因此在加密的选择上应该寻找破解困难的，例如 DES 加密方法，这是一套没有逆向破解的加密算法，因此黑客得到了这种加密处理后的文件时，只能采取暴力破解法。个人用户如果设置了一个复杂的密码，那么黑客的破解工作将会非常艰巨。

7）安装安全软件

网络管理员应在服务器安装必要的安全软件，杀毒软件和防火墙都是必不可少的。在连接网络之前，事先运行这些安全软件，即使遭遇黑客的攻击，物联网系统也具有较强的防御能力。

5.1.5 计算机病毒的防护

1. 计算机病毒的概念

计算机病毒是编制者在计算机程序中插入的破坏计算机网络功能或者数据的代码，能影响计算机网络的使用，能自我复制的一组计算机指令或者程序代码。

计算机病毒具有传染性、繁殖性、潜伏性、隐蔽性、可触发性和破坏性等特征。计算机病毒的生命周期包括：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。

计算机病毒是一个程序，或一段可执行的代码。就像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够通过计算机网络快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或通过网络从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

计算机病毒与医学上的“病毒”不同，计算机病毒不是天然存在的，而是程序员利用计算机网络软件和硬件所固有的脆弱性编制的一组指令集或程序代码。它能潜伏在计算机的存储介质（或程序）里，条件满足时即被激活，通过修改其他程序的方法将病毒代码的精确复制或者可能演化的形式放入其他程序中。从而感染其他计算机程序，对计算机资源进行破坏。因此，计算机病毒是人为编写的恶意程序，对其他网络用户的危害性极大。

2. 计算机病毒的特征

1）传染性

计算机病毒传染性是指计算机病毒通过修改别的程序将自身的复制品或其变体传染到

其他无毒的对象上，这些对象可以是一个程序也可以是系统中的某一个部件。

2）繁殖性

计算机病毒可以像生物病毒一样进行繁殖，当正常程序运行时，它也进行自身复制，是否具有繁殖、感染的特征是判断某段程序为计算机病毒的首要条件。

3）潜伏性

计算机病毒的潜伏性是指计算机病毒可以依附于其他媒体寄生的能力，侵入后的病毒潜伏到条件成熟才发作，会使计算机变慢。

4）隐蔽性

某些计算机病毒具有很强的隐蔽性，不容易被反病毒软件检查出来，隐蔽性计算机病毒时隐时现、变化无常，这类病毒处理起来非常困难。

5）可触发性

编制计算机病毒的人，一般都为病毒程序设定了一些触发条件，例如，系统时钟到达某个特定的日期，或者系统运行了某个特定的程序等。一旦触发条件满足，计算机病毒就会"发作"，对系统进行破坏。

6）破坏性

计算机病毒发作时，会对计算机的软件或硬件进行破坏。例如，可能会导致正常的程序无法运行，也可能把计算机内的重要文件删除或篡改，甚至可能会破坏硬盘中的引导扇区、破坏 BIOS，使计算机无法正常工作。

3. 计算机病毒的分类

计算机病毒种类繁多而且复杂，按照不同的方式以及计算机病毒的特点及特性，可以有多种不同的分类方法。同时，根据不同的分类方法，同一种计算机病毒也可以属于不同的计算机病毒种类。

1）根据计算机病毒寄存的媒体来分类

根据计算机病毒寄存的媒体来分类，可分为网络病毒、文件病毒和引导型病毒三类。

(1) 网络病毒：网络病毒通过计算机网络传播，感染网络中的可执行文件。

(2) 文件病毒：文件病毒感染计算机系统中的文件(如 COM、EXE、DOC 等)。

(3) 引导型病毒：感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。

此外，还有以上三种病毒的混合型病毒，例如：多型病毒(文件和引导型)同时感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2）根据病毒传染渠道来分类

根据病毒传染渠道来划分，可以分为驻留型病毒和非驻留型病毒两类。

(1) 驻留型病毒：这种病毒感染计算机后，把自身的内存驻留部分放在内存(RAM)中，这一部分程序挂接系统调用并合并到操作系统中去，它处于激活状态，一直到关机或重新启动。

(2) 非驻留型病毒：这种病毒在得到机会激活时并不感染计算机内存，一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

3）根据病毒的破坏能力来分类

根据病毒的破坏能力可以分为无害型病毒、无危险型病毒、危险型病毒和非常危险型病

毒四大类。

(1) 无害型病毒：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

(2) 无危险型病毒：这类病毒仅仅是减少内存、显示图像、发出声音及同类影响。

(3) 危险型病毒：这类病毒在计算机系统操作中造成严重的错误。

(4) 非常危险型病毒：这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

4) 根据计算机病毒所使用的算法来分类

根据计算机病毒所使用的算法来划分，可以分为伴随型病毒、“蠕虫”型病毒、寄生型病毒、练习型病毒、诡秘型病毒和变型病毒等类型。

(1) 伴随型病毒：这类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名(COM)，例如，XCOPY. EXE 的伴随体是 XCOPY-COM。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行到，再由伴随体加载执行原来的 EXE 文件。

(2) “蠕虫”型病毒：通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，计算机将自身的病毒通过网络发送。有时它们也会在系统中存在，一般来说，除了内存以外，“蠕虫”型病毒不占用其他资源。

(3) 寄生型病毒：除了伴随和“蠕虫”型，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

(4) 练习型病毒：病毒自身包含错误，不能进行很好的传播，例如一些病毒只在调试阶段。

(5) 诡秘型病毒：它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等对 DOS 内部进行修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

(6) 变型病毒：又称为幽灵病毒，这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的做法是一段混有无关指令的解码算法和被变化过的病毒体组成。

4. 计算机病毒的防治

任何计算机病毒都会对物联网系统构成威胁，但只要培养良好的预防病毒意识，并充分发挥杀毒软件的防护能力，完全可以将大部分病毒拒之门外。

为了保证物联网的正常运行，阻止计算机病毒或者流氓软件入侵物联网系统，物联网用户应当采取以下防御措施：

1) 不要随便浏览陌生的网站

物联网用户不要随便浏览陌生的网站，目前在许多钓鱼式网站中，存在有各种各样的恶意代码，这些亚意代码会危害浏览者电脑的安全。

2) 安装杀毒软件

安装最新版本的杀毒软件，可以防范大多数病毒的攻击。值得注意的是，物联网用户还要及时对杀毒软件进行升级，不断更新病毒资料库，以加强物联网系统的防御能力。

3）安装防火墙

有些物联网用户过于乐观，认为只要安装了杀毒软件，物联网就可以安忧无忧了。但是实际上，安装杀毒软件并不能确保系统绝对安全。目前，除了计算机病毒，物联网网络还可能面临黑客攻击、木马攻击以及间谍软件攻击等多种安全威胁。因此，物联网系统还要安装防火墙。

正如本章5.1.2小节所述，防火墙是根据检查经过网络的数据包来进行监控的，通俗地说，防火墙就相当于一个严格的门卫，守护着物联网系统的大门。防火墙可以把物联网系统的每个端口都隐藏起来，让黑客找不到入口，自然也就保证了系统的安全。

4）及时安装系统漏洞补丁

有经验的网络管理员都会及时运行Windows系统自带的Windows Update程序或杀毒软件自带的漏洞扫描和补丁修复程序，在线更新操作系统。系统安全漏洞扫描工具会及时发现操作系统存在的安全漏洞，并自动下载和安装相应的漏洞补丁程序。

5）不要轻易打开陌生的电子邮件附件

目前，电子邮件病毒也十分猖狂。因此，用户在接收电子邮件时也应当非常小心，千万不要轻易打开陌生的电子邮件的附件，更不要随便回复陌生人的邮件。当收到电子邮件时，应首先用杀毒软件对电子邮件附件进行病毒扫描，以策安全。

6）使用U盘时要先杀毒

除了计算机网络以外，U盘也是传播计算机病毒的主要途径。别人的计算机已经感染了计算机病毒，当用U盘从这台计算机复制文件时，就很可能也感染病毒。因此，使用U盘复制外来的文件时都要先进行杀毒，以防U盘携带病毒传染计算机。

7）对下载的文件进行杀病毒

从网络上下载的文件虽然方便，但也潜伏着危机。因此，用户从网络上下载了任何文件之后，一定要先对文件进行病毒扫描，确认无病毒之后才运行。

8）及时备份

备份是一种有效的防护措施，用户对于重要的文件一定要做及时做好备份，以免系统遭到病毒破坏后不能恢复，造成不必要的损失。对于已经感染病毒的计算机，可以下载最新的杀毒软件进行清除。目前，国内常见的杀毒软件都终身免费，如金山毒霸、江民杀毒、瑞星杀毒和360杀毒等。

5.1.6　入侵检测技术

1. 入侵检测技术概述

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。进行入侵检测的软件与硬件相结合，便构成入侵检测系统（Intrusion Detection System，IDS）。

入侵检测系统可以被定义为对计算机和网络资源的恶意使用行为进行识别和相应处理的系统。包括系统外部的入侵和内部用户的非授权行为，是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计

算机网络中违反安全策略行为的技术。

入侵检测的内容包括：试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户信息的泄漏、独占资源以及恶意使用。进行入侵检测的硬件与软件的整体便是入侵检测系统。它通过从计算机网络或计算机系统的关键点收集信息并进行分析，发现计算机网络或计算机系统中是否有违反安全策略的行为和被攻击的迹象，并且针对攻击行为作出反应。

入侵检测被认为是企业网除了防火墙技术之外另一道安全闸门，它提供对内部攻击、外部攻击和误操作的实时保护。这些都可以通过以下方法来实现：

(1) 监视、分析用户及系统活动，防止非法用户和合法用户的越权操作；

(2) 系统构造和弱点的审计，提示管理员及时修补安全漏洞；

(3) 识别反映已知进攻的活动模式并向管理员报警；

(4) 异常行为模式的统计分析，发现入侵行为的规律；

(5) 评估重要系统和数据文件的完整性；

(6) 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

2. 入侵检测的过程

入侵检测的过程可以分为三个步骤：信息收集、信息分析和结果处理。

1) 信息收集

入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息，包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

2) 信息分析

收集到的有关系统、网络、数据及用户活动的状态和行为等信息，被送到检测引擎，检测引擎驻留在传感器中，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。当检测到某种误用模式时，产生一个告警并发送给控制台。

3) 结果处理

控制台按照告警产生预先定义的响应采取相应措施，相应措施可以是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的告警。

3. 入侵检测系统的结构

一个典型的入侵检测系统的结构如图 5-4 所示。

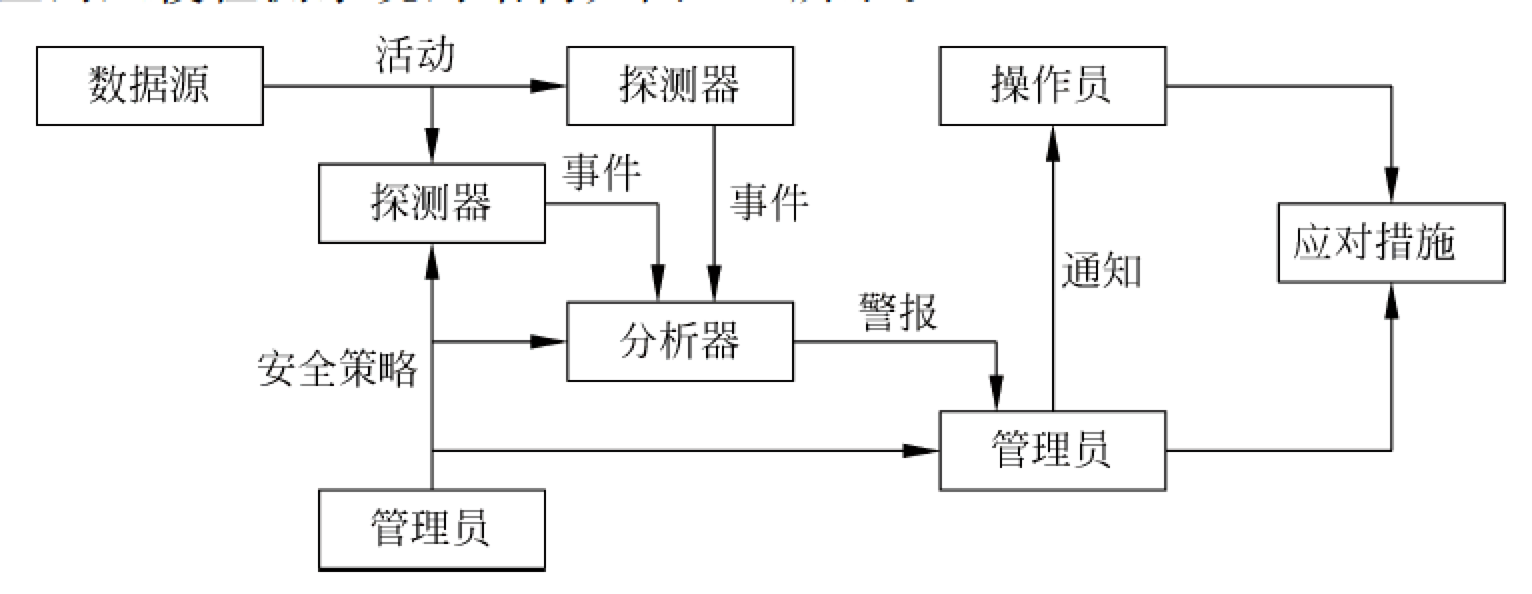


图 5-4　入侵检测系统的结构

1）数据源

数据源为入侵检测系统提供最初的数据来源，系统利用这些数据来检测入侵。数据源包括网络包、审计日志、系统日志和应用程序日志等。

2）探测器

探测器从数据源提取出与安全相关的数据和活动，例如非法的网络连接或用户的越权访问等，并将这些数据传送给分析器作进一步的分析。

3）分析器

分析器的职责是对探测器送来的数据进行分析，如果发现未授权或非法行为，就产生警报并报告给管理器。

4）管理器

管理器是入侵检测系统的管理部件，其主要功能是配置探测器、分析器；通知管理员发生了入侵；采取应对措施等。管理器接收到分析器的警报后，便通知管理员并报告情况，通知的方式有声音、电子邮件等。同时管理器还可以主动地采取应对措施，例如结束进程、切断连接、改变文件和网络的访问权等。管理员利用管理器来管理入侵检测系统，并根据管理器的报告采取进一步的措施。

5）管理员

管理员是网络和计算机系统的管理者，负责制定安全策略和部署入侵检测系统。

6）安全策略

安全策略是预先定义的一些规则，这些规则规定了网络中哪些活动允许执行和哪些主机可以访问内部网络等。安全策略通过应用到探测器、分析器和管理器上来发挥作用。

4. 入侵检测技术的分类

入侵检测技术可以分为异常检测和误用检测两大类。

1）异常检测（Anomaly Detection）

异常检测技术能够检测出可接受行为与不可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不可接受的行为就应该是入侵。首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型漏报率低，误报率高。因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵。

2）误用检测（Misuse Detection）

误用检测技术能够检测用户行为与已知的不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起告警。这种技术事先收集不正常的操作行为的特征，建立不可接受行为特征库。当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率比较低，但是漏报率比较高。对于已知的攻击行为，它可以详细、准确地检测到攻击，但是对未知攻击却效果有限，而且不可接受行为特征库必须不断更新。

5. 入侵检测方法

常用的入侵检测系统检测方法有特征检测、统计检测和专家系统。目前，大多数入侵检测系统都采用入侵模板进行模式匹配的特征检测系统，有些采用基于统计模型的入侵检测

系统，有些采用基于日志的专家知识库系统。除此以外，还有基于内核的入侵检测系统、基于免疫系统的入侵检测系统、基于遗传算法的入侵检测系统、蜜罐和蜜网等。

1）基于特征检测的入侵检测系统

特征检测系统对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时，立即报警。其工作原理与专家系统相似，检测方法与计算机病毒的检测方式相似。该方法检测的准确率比较高，但对于无经验知识的入侵和攻击行为无能为力。

2）基于统计模型的入侵检测系统

统计模型常用于异常检测。在统计模型中，常用的检测参数包括：审计事件的数量、间隔时间和资源消耗的情况等。常用的入侵检测的统计模型包括：马尔科夫过程模型和时间序列分析模型。这种入侵检测方法是基于对用户历史行为建模以及在早期的证据及模型的基础上，审计系统实时检测用户对系统的使用情况，根据系统内部保存的用户行为概率统计模型进行检测，一旦发现有可疑的用户行为时，就会保持跟踪并监测、记录该用户的行为。

统计方法的最大优点是它可以“学习”用户的使用习惯，从而具有较高检出率和可用性。然而它的“学习”能力也给了入侵者机会，入侵者可以通过“训练”使入侵事件符合正常操作的统计规律，从而达到入侵的目的。

3）基于专家知识库的入侵检测系统

专家知识库系统对入侵进行检测，经常是针对具有某种特征的入侵行为。这种检测技术根据安全专家对可疑行为的分析经验形成一套推理规则，然后在此基础上建立相应的专家知识库系统。据此，专家系统自动对所涉及的入侵行为进行分析。并且，专家知识库系统能够随着经验的积累而利用其自学能力进行规则的补充及修正。

在专家知识库系统中，所谓的规则即是知识，不同的系统与设置具有不同的规则，而且规则之间没有通用性。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性和实时性。入侵的特征抽取和表达是入侵检测专家系统的关键。

4）基于内核的入侵检测系统

随着开放源代码的操作系统 Linux 的流行，基于内核的入侵检测成为检测领域的新方法。这种方法的核心是从操作系统的层次上看待安全漏洞，采取措施避免甚至杜绝安全隐患。这种方法主要是通过修改操作系统源代码或者向内核中加入安全模块来实现的，可以保护重要的系统文件和进程。

5）基于免疫系统的入侵检测系统

与生物学中的免疫系统类似，基于免疫系统的入侵检测系统是保护生命机体不受病原体侵害的系统，它对病原体和非自身组织的检测相当准确。不但能够记忆曾经感染过的病原体的特征，还能够有效地检测未知的病原体。免疫系统具有分层保护、分布式检测、各部分相互独立和检测未知病原体的特性，这些都是计算机信息安全系统所缺乏和迫切需要的。

免疫系统最重要的能力是识别自我和非我的能力，这个概念与入侵检测技术中的异常检测的概念很相似。因此，有些学者从免疫学的角度对入侵检测系统进行研究。

6）基于遗传算法的入侵检测系统

遗传算法是进化算法的一种，它引入了达尔文在进化论里提出的自然选择概念，对入侵检测系统进行优化。遗传算法利用对“染色体”的编码和相应的变异和组合，形成新的个体。

遗传算法通常对需要优化的系统变量进行编码,作为构成个体的“染色体”,再利用相应的变异和组合,形成新的个体。

对于遗传算法的研究者来说,入侵的检测过程可以抽象为:为审计记录定义一种向量表示形式,这种向量或者对应于攻击行为,或者表示正常行为。通过对所定义的向量进行测试,提出改进的向量表示形式,并且不断重复这个过程,直到得到令人满意的结果。

7)蜜罐

蜜罐也是一种入侵检测系统,设计者诱导攻击者访问预先设置的蜜罐,而不是工作中的网络,从而提高检测攻击和攻击者行为的能力,降低攻击带来的破坏。

设计蜜罐的目标有两个:一是在不被攻击者察觉的情况下监视他们的活动、收集与攻击者相关的所有信息;二是牵制攻击者,使之将时间和精力都耗费在攻击蜜罐上,从而远离实际的工作网络。

8)蜜网

蜜网的概念是由蜜罐发展起来的。早期人们为了研究黑客的入侵行为,在网络中放置了一些特殊的计算机,并且在这些计算机上运行专用的模拟软件,使得从外界看来这些计算机就是网络上运行某些操作系统的主机。将这些计算机连接入网络,并为其设置较低的安全防护等级,诱使入侵者进攻系统。入侵者进攻系统后,一切行为都会被系统软件监控和记录,通过系统软件收集描述入侵者行为的数据,就可以对入侵者的行为进行分析。

目前,蜜网的软件产品已经很多,可以模拟各种不同的操作系统,例如:Windows、RedHat、FreeBSD、Cisco 路由器的 IOS 等。然而,模拟软件并不能完全反映真实的网络状况,也不可能模拟实际网络中所出现的各种情况。在其之上收集到的数据有一定的局限性,因此,又出现了用真实的计算机组建的蜜网。

5.1.7 网络安全扫描技术

1. 网络安全扫描技术概述

随着网络攻击技术的发展,攻击工具和方法日趋复杂,网络攻击已构成对网络安全极大的威胁。网络攻击的一个重要特征就是具有阶段性。在准备阶段,网络攻击者要进行情报的搜集与分析工作;在攻击实施阶段要进行远程登录、远程攻击、取得普通用户权限甚至超级用户权限等工作;在善后处理阶段则需要设置“后门”和清除日志等一系列后续工作。

利用扫描工具对目标系统进行扫描,找到目标系统的漏洞和脆弱点,是实施网络攻击的第一步,这对网络攻击者来说是至关重要的。同样,对于进行网络防御的管理员来说,首先要做的就是利用扫描工具探测自身网络的安全隐患,及时发现漏洞,在被攻击之前进行相应的防范和补救来提高网络的安全性,防患于未然。

扫描工具是一种利用网络安全扫描技术自动地检测目标主机安全弱点的程序。它能够发现目标主机开放的端口和运行的服务,是否存在系统漏洞和安全弱点等。它通过与目标主机开放的端口建立连接或请求服务,如 http、telnet 等,获取目标主机的应答信息,以搜集相关的信息,如操作系统类型等,从而发现目标主机存在的安全弱点。它是一把双刃剑,利用网络安全扫描工具的扫描结果,可以为攻击目标网络系统提供指导,同时还可以用于网络系统的安全评测,评估网络系统的安全性,对系统存在的漏洞提出修补建议。因此,网络安

全扫描工具既是网络攻击的重要武器之一，同时也是网络安全防御的重要手段之一。

鉴于网络安全扫描技术的双面性，对其进行深入的研究不仅可以更好地为网络安全服务，而且可以深刻认识黑客攻击，从而做到主动防御。目前，网络安全扫描技术已成为网络安全问题研究的一个重要组成部分，有着非常重要的实用价值。

2. 网络安全扫描技术分析

目前，网络安全扫描技术主要包括端口扫描技术、弱密码扫描技术、操作系统探测技术以及漏洞扫描技术等。

1）端口扫描技术

一个开放的端口就是一个潜在的通信通道，也是一个入侵的通道。对目标计算机进行端口扫描，可以得到许多有用的信息，如开放端口及所提供的服务等。端口扫描是向目标主机的 TCP 或 UDP 端口发送探测数据包，记录目标主机的响应，然后通过分析响应数据包来判断端口是否开放以及所提供的服务或信息，帮助我们发现主机存在的某些安全隐患。它为系统用户管理网络提供了一种手段，同时也为网络攻击提供了必要的信息。

目前，端口扫描的方式主要包括 TCP 全连接扫描和 TCP 半连接扫描。

（1）TCP 全连接扫描。

TCP 全连接扫描的过程是先向目标主机端口发送 Syn 报文，然后等待目标端口发送 Syn/Ack 报文，收到后再向目标端口发送 Ack 报文，即著名的“三次握手”过程。在许多系统中只须调用一个 connect 函数即可完成。该方法的方便之处在于它不需超级用户权限，任何希望管理端口服务的人都可以使用，但它通常会在目标主机上留下扫描记录，易被管理员发现。

（2）TCP 半连接扫描。

TCP 半连接扫描通常被称为“半开放”式扫描。扫描程序向目标主机端口发送一个 Syn 数据包，一个 Syn/Ack 的返回信息表示端口处于侦听状态，而一个 Rst 的返回信息，则表示端口处于关闭状态。由于它建立的是不完全连接，所以通常不会在目标主机上留下记录，但构造 Syn 数据包必须要有超级用户权限。

除此之外，还有 TCP Fin 扫描、UDP 扫描、ICMP Echo 扫描、Ack 扫描以及窗口扫描等，这里不再赘述。

2）弱密码扫描技术

（1）密码与弱密码。

所谓密码，它为用户的数据安全提供了必要的安全保障。如果一个用户的密码被非法用户获得，则非法用户就获得了该用户的权限，尤其是最高权限用户的密码泄漏以后，主机和网络也就失去了安全性。通过密码进行身份认证是目前实现计算机安全的主要手段之一。

弱密码即为弱势密码，指易于猜测、破解或长期不变更的密码，比如 123 和 sa 等比较简单的密码。有些密码虽然不简单，但容易被人猜到，如网络管理员的姓名、生日等，也属于弱密码。弱密码的存在是非常危险的，很容易被非法用户破解。

（2）暴力破解。

密码检测是网络安全扫描工具的一部分，它要做的就是判断用户密码是否为弱密码。如果存在弱密码，则提醒管理员或用户及时修改。所谓的暴力破解就是暴力密码猜测，是攻

击者试图登录目标主机，不断输入密码，直到登录成功为止的攻击方法。它只需要能连接到目标主机的可登录端口，然后通过人工或自动执行工具软件一次次地猜测来进行判断，速度较慢。这种看似笨拙的方法却是黑客们最常用的方法，也往往是最有效的方法之一。它针对的是弱密码，而用户弱密码是普遍存在的。

黑客的暴力破解是对用户密码强度的考验，那么，在接受黑客考验之前，用黑客的方法先对密码强度进行检测，确保其可靠性，就会大大降低暴力破解的成功率。因此，弱密码扫描是网络安全扫描必不可少的环节。

3）操作系统探测技术

操作系统类型是进行入侵或安全检测需要收集的重要信息之一。绝大部分系统安全漏洞都与操作系统有关，因此，探测出目标主机操作系统的类型甚至版本信息对于攻击者和网络防御者来说都具有重要的意义。目前流行的操作系统探测技术主要有应用层探测技术和TCP/IP 协议栈指纹探测技术。

应用层探测技术是通过向目标主机发送应用服务连接，或访问目标主机开放的有关记录，探测出目标主机的操作系统信息，如通过向服务器请求 Telnet 连接，可以知道运行的操作系统类型和版本信息。其他的如 Web 服务器、DNS 主机记录、SNMP 等也可以提供相关的信息。

TCP/IP 协议栈指纹探测技术是利用各种操作系统在实现 TCP/IP 协议栈时存在的一些细微差别，通过探测这些细微的差异，来确定目标主机的操作系统类型。主动协议栈指纹技术和被动协议栈指纹技术是目前探测主机操作系统类型的主要方式。

（1）主动协议栈指纹技术。

这种技术主要是主动有目的地向目标系统发送探测数据包，通过提取和分析响应数据包的特征信息，来判断目标主机的操作系统信息。主要有 Fin 探测分组、假标志位探测、ISN 采样探测、TCP 初始化窗口、ICMP 信息引用、服务类型以及 TCP 选项等。

（2）被动协议栈指纹技术。

这种技术主要是通过被动地捕获远程主机发送的数据包来分析远程主机的操作系统类型及版本信息，它比主动方式更隐秘，一般可以从四个方面着手：TTL、WS、DF 和 TOS。在捕捉到一个数据包后，通过综合分析上述四个因素，就能基本确定一个操作系统的类型。

4）漏洞扫描技术

漏洞是硬件、软件或者安全策略上的错误而引起的缺陷，从而使别人能够利用这个缺陷在未经授权的情况下访问系统或者破坏系统的正常使用。漏洞的种类很多，主要有网络协议漏洞、配置不当导致的系统漏洞和应用系统的安全漏洞等。

漏洞扫描技术是自动检测远端或本地主机安全脆弱点的技术。根据安全漏洞检测的方法，可以将漏洞扫描技术分为以下四种类型：

（1）基于主机的检测技术。

基于主机的检测技术主要检查一个主机系统是否存在安全漏洞。这种检查将涉及操作系统的内核、文件属性、操作系统补丁和不合适的设置等问题。

（2）基于网络的检测技术。

基于网络的检测技术主要检查一个网络系统是否存在安全漏洞以及抗攻击能力。它运行于单个或多个主机，可以采用常规漏洞扫描的方法来检查网络系统是否存在安全漏洞，也

可以采用仿真攻击的方法来测试目标系统的抗攻击能力。

(3) 基于审计的检测技术。

基于审计的检测技术主要通过审计一个系统的完整性来检查系统内是否存在被故意安放的后门程序。这种安全审计将周期性地使用单向散列算法对系统的特征信息如文件的属性等进行计算,并将计算结果与初始计算结果相比较,一旦发现改变就通知管理员。

(4) 基于应用的检测技术。

基于应用的检测技术主要利用软件测试的结果检查一个应用软件是否存在安全漏洞,如应用软件的设置是否合理、有无缓冲区溢出问题等。

3. 网络安全扫描技术的发展

网络的不安全性激发了研究者对网络安全防护技术的广泛关注。在网络攻击者与网络安全技术人员之间的攻防战不断升级过程中,出现了多种多样的网络安全技术和防护工具。

网络安全扫描是众多的网络安全技术之一,是解决网络安全问题的另一种思路。网络安全扫描技术最早由 Dan Farmer 和 Weitse Venema 等人在 1995 年提出并实现,其基本思想是模仿入侵者的攻击方法,从攻击者的角度来评估网络系统的安全性。他们开发的 SATAN 扫描工具是一个运行在 Linux 环境下的端口扫描程序,虽然功能比较简单,但它体现了这样一种观点:一个网络管理员能够保障系统安全的途径之一,是分析入侵者是如何侵入系统的。这种安全扫描方式,能够更准确地向网络管理员报告系统中存在安全问题的地方,以及需要加强安全管理的地方,这种方法比其他方法更具有指导性和针对性。

在实际应用中,网络安全扫描主要用来搜集网络信息,帮助我们发现目标主机的弱点和漏洞,并能根据扫描结果提高网络安全性能,防范黑客攻击。网络安全扫描工具通常应具备以下几种功能:

(1) 能够发现一台主机或一个网络。

(2) 对于正在运行的主机,能够发现主机开放的端口及提供的服务,能够较为准确地探测出主机运行的操作系统类型及版本信息。

(3) 通过探测系统和服务,能够发现系统中存在的安全漏洞。

网络安全扫描工具一直是网络安全界的研究热点,国内外的一些研究人员也一直致力于这方面的研究。目前研究成果主要有国外的 Nmap、SuperScan、Nessus 等,以及国内的 X-Scan 和流光等。

Nmap 是 Fyodor 编写的网络安全扫描工具。它提供了比较全面的扫描方法,如支持 TCP、UDP 等多种协议的扫描方式,以及利用协议栈指纹技术识别目标主机操作系统的功能,是目前国内外最为流行的端口扫描工具之一。Nmap 虽然是一个强大的端口扫描工具,但它没有漏洞扫描的功能,无法对目标主机的脆弱性进行深入挖掘,不符合网络攻击系统中综合性能强的作战要求。

SuperScan 是 Robin Keir 编写的应用在 Windows 环境下的 TCP 端口扫描程序。它允许用户灵活的定义目标主机的端口列表,而且图形化的交互界面使用起来比较简单方便。

Nussus 是一款运行在 Linux、BSD、Solaris 以及其他系统上的安全扫描工具,是一款基于多线程和插件的漏洞扫描软件。该软件具有漏洞数据与 CVE 标准兼容的特性,能够完成超过 1200 项的远程安全检查,具有强大的报告输出能力,并且会为每个发现的安全问

题提出解决建议。

X-Scan 是国内“安全焦点”编写的一个运行于 Windows 环境下的安全漏洞扫描工具。它采用多线程方式对指定 IP 地址段进行安全漏洞扫描，支持插件功能，提供了图形化界面和命令行两种操作方式，实现对远程主机的操作系统类型、标准端口以及常见漏洞的扫描。但它只提供了一种端口扫描方式，在目标网络复杂时无法灵活自主地进行选择配置，从而限制了它的适用性。

流光是国内著名网络安全专家小榕所开发的扫描工具，它除了能够像 X-Scan 那样扫描众多的漏洞和弱密码外，还集成了其他的入侵工具，如字典工具、NT/IIS 工具等。另外，还独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。虽然它的功能多一些，但操作起来非常繁杂。

通过对国内外的网络安全扫描工具的分析和了解可以看出，现在的扫描工具都有各自的特点和局限性。而我国开展网络安全扫描技术的研究工作起步比较晚，工作不够深入，系统性和综合性不强。鉴于扫描技术在当前网络安全问题中的重要地位，必须深入开展网络安全扫描关键技术研究，才能更好地做好网络安全防护工作。

5.2　无线网络安全技术

根据工作原理来区分，无线网络可以分为无线局域网（WLAN）、无线城域网（WiMAX）、蓝牙网络（Bluetooth）、ZigBee 网络、超宽带网络（UWB）、WMN 网络等类型。

5.2.1　无线局域网安全

无线局域网一般用于较小范围的无线通信，覆盖范围比较小，一般为一栋建筑物内或房间内，采用 IEEE 802.11 系列标准，其传输速率一般在 11～300Mbps 之间，传输距离一般为 50 米～100 米，工作频段为 2.4GHz。

IEEE 802.11 系列标准包括 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 和 IEEE 802.11n 等几个重要标准，主要用于实现企业内部网络用户终端或者家庭无线网络用户的近距离无线接入，即 Wi-Fi 接入。

无线局域网具有安装简单、使用方便、经济节约、易于扩充等有线网络无法比拟的优点，因此得到了越来越广泛的使用。然而，无线局域网信道开放的特点使得攻击者能够很容易地进行窃听、恶意修改并转发，因此安全性成为阻碍无线局域网发展的最重要因素。虽然对无线局域网的需求不断增长，但是安全问题也让许多潜在的用户望而却步，对最终是否采用无线局域网系统犹豫不决。

1. 无线局域网的安全威胁

使用无线局域网实现网络通信时，网络必须具有较强的保密能力。目前市场上的无线局域网产品，主要存在以下安全威胁：

1）容易被入侵

无线局域网非常容易被发现，为了能够使用户发现无线网络的存在，无线网络必须发送有

特定参数的信标帧，因此就给攻击者提供了必要的网络信息。攻击者可以通过高灵敏度天线从公路边、楼房中以及其他任何地方对无线网络发起攻击而不需要任何物理方式的连接。

2）存在非法接入点

无线局域网易于访问和配置简单的特性，常常使得网络管理员非常苦恼。因为如果不设置密码，任何人都可以通过手机或者电脑不经授权而接入无线局域网。而且，有许多部门并没有经过企业信息中心的授权，就自行组建无线局域网，这种非法的无线接入点会给整个物联网带来很大的安全隐患。

3）未经授权使用服务

几乎有一半以上的网络用户，在配置无线接入点时，仅仅进行简单的配置。几乎所有的无线接入点都按照默认配置来开启 WEP 进行加密或者使用原厂提供的默认密钥。由于无线局域网开放式的访问方式，因此未经授权用户擅自占用网络资源时，不仅会增加带宽费用，还有可能导致法律纠纷。未经授权的用户并没有遵守服务提供商提出的服务条款，这很可能会导致 ISP 中断服务。

4）服务和性能的限制

无线局域网的传输带宽是有限的，由于物理层的开销，使得无线局域网的实际最高有效吞吐量仅仅为标准的一半，而且该带宽是被无线接入点的所有用户共享的。无线带宽可以被多种方式占用，比如来自有线网络远远超过无线网络带宽的网络流量，如果攻击者从快速以太网发送大量的 ping 信号，就可以轻易地占用无线接入点有限的带宽。

5）地址欺骗和会话拦截

由于 802.11 无线局域网对数据帧不进行认证操作，使得攻击者可以通过欺骗重新定向数据流，使 ARP 表变得混乱。通过非常简单的方法，攻击者就可以轻易获得无线网络中站点的 MAC 地址，这些地址可以在恶意攻击时使用。

6）流量分析与流量侦听

802.11 无线局域网无法防止攻击者采用被动方式监听网络流量，而任何无线网络分析设备都可以不受任何阻碍的截获未进行加密的网络流量。目前，WEP 存在可以被攻击者利用的漏洞，它只能保护用户和网络通信的初始数据，管理和控制帧是不能被 WEP 加密和认证的。显然，这就给攻击者以欺骗帧终止网络通信提供了机会。

7）高级入侵

一旦攻击者进入无线局域网，它将成为进一步入侵其他系统的起点。很多无线网络都有一套精心设置的安全设备作为网络的外壳，以防止非法攻击。但是在外壳保护的网络内部却非常脆弱，很容易受到攻击。无线网络通过简单配置就可以快速的接入主干网络，这将使得网络暴露在攻击者面前，从而遭到入侵。

2. 无线局域网安全技术

到目前为止，已经出现了多种无线局域网的安全技术，包括物理地址过滤、服务区标识符（SSID）匹配、有线对等保密（WEP）、端口访问控制技术、WPA、IEEE 802.11i 和 WAPI 等。

1）物理地址（MAC）过滤

每一个无线工作站网卡都有唯一的 48 位二进制数的物理地址（MAC），该物理地址编

码方式类似于以太网的物理地址。网络管理员可以在无线局域网访问点(Access Point, AP)中手工维护一组允许(或不允许)通过 AP 访问网络地址的列表,以实现基于物理地址的访问过滤。

物理地址过滤具有如下四个优点:

(1) 简化了访问控制。

(2) 接受或者拒绝预先设定的用户。

(3) 被过滤的物理地址不能进行访问。

(4) 提供了第二层防护。

然而,物理地址过滤也存在以下两个缺点:

(1) 当 AP 和无线终端数量较多时,大大增加了管理负担。

(2) 容易受到 MAC 地址伪装攻击。

2) 服务区标识符(SSID)匹配

服务区标识符(Service Set Identifier,SSID)匹配将一个无线局域网分为几个不同的子网络,每一个子网络都有其对应的身份标识(SSID),只有无线终端设置了配对的 SSID 才能接入相应的子网络。因此可以认为 SSID 是一个简单的口令,提供了口令认证机制,实现了一定的安全性。但是这种口令很容易被无线终端探测出来,企业级无线应用绝不能只依赖这种技术做安全保障,而只能作为区分不同无线服务区的标识。

3) IEEE 802.11 WEP 加密技术

IEEE 802.11 标准定义了一种称为有线对等保密(WEP)的加密技术,其目的是为无线局域网提供与有线网络相同级别的安全保护。WEP 采用静态的有线对等加密密钥的基本安全方式。静态 WEP 密钥是一种在会话过程中不发生变化,也不针对各个用户而变化的密钥。在标准中,加密密钥长度有 64 位和 128 位两种。其中 24 位的加密密钥是由系统产生的,因此需要在无线接入点和无线站点上配置的密钥只有 40 位或 104 位。

IEEE 802.11 WEP 在传输上提供了一定的安全性和保密性,能够阻止无线用户有意或无意地查看到无线接入点和无线站点之间传输的内容,其主要优点如下:

(1) 全部报文都是使用校验和加密,提供的一些抵抗篡改的能力。

(2) 通过加密来维护一定的保密性,如果没有密钥,就难以对报文解密。

(3) WEP 非常容易实现。

(4) WEP 为无线局域网应用程序提供了非常基本的保护。

然而,IEEE 802.11 WEP 也存在以下 6 个缺点:

(1) 静态 WEP 密钥对于 WLAN 上的所有用户都是通用的。

这意味着如果某个无线设备丢失或者被盗,所有其他设备上的静态 WEP 密钥都必须进行修改,以保持相同级别的安全性。这将给网络管理员带来非常费时费力的、不切实际的管理任务。

(2) 缺少密钥管理。

WEP 标准中并没有规定共享密钥的管理方案,通常是手工进行配置与维护。由于更换密钥的费时与困难,因此密钥通常长时间使用而极少更改。

(3) ICV 算法不合适。

ICV 算法是一种基于 CRC-32 的用于检测传输噪音和普通错误的算法。CRC-32 是信

息的线性函数，这意味着攻击者可以篡改加密信息，并且很容易的修改ICV，使伪装的信息表面上看起来是可信的。

(4) RC4算法存在弱点。

在RC4算法中存在弱密钥。所谓弱密钥，就是密钥与输出之间存在相关性。攻击者收集到足够多的使用弱密钥的数据包后，就可以对弱密钥进行分析，只需尝试很少的密钥就可以接入到无线局域网中。

(5) 认证信息容易伪造。

基于WEP的共享密钥认证的目的就是实现访问控制，但是事实却截然相反。只要通过监听一次成功的认证，攻击者以后就可以伪造认证。启动共享密钥认证实际上降低了网络的总体安全性，使得攻击者猜中WEP密钥变得更为容易。

(6) WEP2算法没有解决其机制本身产生的安全漏洞。

为了提高安全性，Wi-Fi工作组提供了WEP2技术，该技术与WEP算法相比，仅仅是将WEP密钥的长度从四十位加长到一百二十八位，初始化向量的长度从二十四位加长到一百二十八位。但是WEP算法的安全漏洞，是由于WEP安全机制本身引起的，与密钥的长度无关，尽管增加了密钥的长度，也不可能增强其安全程度。也就是说，WEP2算法并没有起到提高安全性的作用。

4) IEEE 802.1x/EAP用户认证

IEEE 802.1x是针对以太网而提出的基于端口进行网络访问控制的安全性标准。基于端口的网络访问控制利用物理层特性对连接到局域网端口的设备进行身份认证。如果认证失败，则禁止该设备访问局域网的资源。

尽管IEEE 802.1x标准最初是为有线局域网设计和制定的，但是它也适用于符合IEEE 802.1x标准的无线局域网，并且被视为无线局域网的一种增强性网络安全解决方案。IEEE 802.1x的体系结构包括以下三个主要的组件。

(1) 请求方：提出认证申请的用户接入设备，在无线局域网中，通常只接入网络的无线客户端设备。

(2) 认证方：允许客户端进行网络访问的实体，在无线局域网中，通常指访问接入点(AP)。

(3) 认证服务器：为认证方提供认证服务的实体。认证服务器对认证方进行验证，然后告知认证方该请求者是否为授权用户。认证服务器可以是某个单独的服务器实体，也可以不是单独的服务器实体，此时通常都是将认证功能集成到认证方。

IEEE 802.1x标准为认证方定义了两种访问控制端口，即受控端口和非受控端口。受控端口分配给那些已经成功通过认证的实体进行网络访问；而认证尚未完成之前，所有的通信数据流从非受控端口进出。非受控端口只允许通过IEEE 802.1x认证的数据，一旦认证成功通过，请求方就可以通过受控端口访问无线局域网的资源和服务。

IEEE 802.1x技术是一种增强型的网络安全解决方案。在采用的IEEE 802.1x无线局域网中，无线用户端安装客户端软件作为请求方，无线访问点(AP)嵌入IEEE 802.1x认证代理作为认证方，同时它还作为RADIUS认证服务器的客户端，负责用户与RADIUS服务器之间认证信息的转发。

5) WPA(IEEE 802.11i)标准

针对人们对提高无线局域网安全的迫切需求，Wi-Fi联盟专门制定了Wi-Fi保护接入

标准(Wi-Fi Protected Access,WPA)。WPA 是 IEEE 802.11i 的一个子集,其核心就是 IEEE 802.1x 和 TKIP。

WPA 采用了 IEEE 802.1x 和 TKIP 来实现无线局域网的访问控制、密钥管理和数据加密。尽管 WPA 在安全性方面比 WEP 有了很大的改进和加强,但是 WPA 仅仅是一个临时性的过渡方案,WPA2 则进一步采用了 AES 加密机制。

IEEE 802.11i 是新一代的无线局域网安全标准。为了使无线局域网技术从安全性得不到很好保障的困境中解脱出来,IEEE 802.11 工作组致力于制订被称为 IEEE 802.11i 的新一代安全标准,这个安全标准是为了增强无线局域网的数据加密和认证性能,定义了强健安全网络(Robust Security Network,RSN)的概念,并且针对 WEP 加密机制的各种缺陷做了多方面的改进。

IEEE 802.11i 安全标准规定使用 IEEE 802.1x 认证和密钥管理方式,在数据加密方面,定义了 TKIP(Temporal Key Integrity Protocol)、CCMP(Counter-Mode/CBC-MAC Protocol)和 WRAP(Wireless Robust Authenticated Protocol)3 种加密机制。其中 TKIP 采用了 WEP 机制中的 RC4 作为核心加密算法,可以通过在现有的设备上升级固件和驱动程序的方法,达到提高无线局域网安全的目的。CCMP 机制基于 AES(Advanced Encryption Standard)加密算法和 CCM(Counter-Mode/CBC-MAC)认证方式,使得无线局域网的安全性能大大提高,是实现 RSN 的强制性要求。

6) WAPI 协议

虽然 IEEE 802.11i 解决了无线局域网传统安全体制的大部分问题,但是当它应用到运营中的无线局域网时,仍然存在相当的问题。

WAPI 协议采用国家密码管理局委员会办公室批准的公开密钥体制的椭圆曲线密码算法和秘密密钥体制的分组密码算法,分别用于无线局域网设备的数字证书、密钥协商以及传输数据的加密和解密,从而实现设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。

WAPI 安全系统采用公钥加密技术,鉴别服务器 AS 负责证书的颁发、验证与吊销等,无线客户端及移动终端与无线接入点 AP 上都安装有 AS 颁发的公钥证书,作为自己的数字身份凭证。当移动终端登录到无线接入点时,在使用和访问网络之前必须通过鉴别服务器对双方进行身份验证。根据验证的结果,持有合法证书的移动终端才能接入持有合法证书的无线接入点,也就是说才能通过无线接入点访问网络。这样不仅可以防止非法移动终端接入而访问网络并占用网络资源,而且还可以防止移动终端登录到非法无线接入点造成的信息泄露。

5.2.2　无线城域网安全

1. 无线城域网概述

无线城域网(Wireless Metropolitan Area Network,WMAN)是指以无线方式构成的城域网,它提供面向互联网的高速连接。WMAN 既可以使用无线电波,也可以使用红外光波来传送数据,它提供给用户以高速访问 Internet 的无线访问网络带宽,其需求正日益增长。

WiMAX 论坛(微波存取全球互通技术论坛)是 2001 年 6 月在美国加州注册的产业界

为主导的非赢利经济组织，宗旨在于促进 WiMAX 在全球发展和产业化应用。WiMAX 论坛推动基于 IEEE 802.16/ETSI HiperMan 标准的宽带无线产品的认证、互通性和兼容性，鼓励所有的无线宽带接入相关产业的厂商遵循一个统一的规范，使各个产品具有良好的互操作性。

IEEE 的 802.16 标准用于标准化空中接口和无线本地环路与耦合的相关功能，它是一种无线城域网的革命性标准，可以为数据、视频和语音业务提供高速的无线接入服务。IEEE 802.16 的主要目的是提供宽带无线接入，因此它被认为是一种取代 xDSL 等有限宽带接入的有力替代者。该标准的主要优势在于可以快速、灵活地进行网络部署，从而降低网络的建设成本。对于城市等人口密集区域和农村等没有有线网络基础的网络建设，无线宽带接入设备的优势是非常明显的。

WiMAX/802.16 网络体系包括：核心网、用户基站(SS)、基站(BS)、中继站(RS)、用户终端设备(TE)和网管。参考模型分为非漫游模式和漫游模式，网络实体包括接入网、连接服务网络；接口 R1 至 R5 为网络工作组初步确定了在 Release1 规范中定义的开放接口，接口 R6 至 R8 为后续版本中考虑开放的接口。

WiMAX/802.16 能够支持多种业务，采用面向连接机制，根据不同业务需求提供端到端的 QoS。IEEE 802.16 定义了四种业务类型，并对每种业务类型的带宽请求方式进行了规定(优先级从高到低)：

(1) 主动授权业务(UGS)；

(2) 实时轮询业务(rtPS)；

(3) 非实时轮询业务(nrtPS)；

(4) 尽力而为(BE)业务。

2. WiMAX/802.16 安全

WiMAX/802.16 标准为无线空中接口分别定义了介质访问控制(MAC)层和物理层。

在 IEEE 802.16 标准中，定义了物理层实现的 5 种方式，即 WMAN—SC、WMAN—SCa、WMAN—OFDM、WMAN—OFDMA 和 WirelessHUMAN。物理层的关键技术有：双工复用方式、载波带宽、OFDM 和 OFDMA、自适应调制、多天线技术等。

MAC 层分成三个子层：汇聚子层(Convergence Sublayer, CS)、公共部分子层(Common Part Sublayer, CPS)、安全子层(Privacy Subayer, PS)。CS 层根据提供服务的不同，提供不同的功能。对于 IEEE 802.16 来说，能提供的服务包括数字音频/视频广播、数字电话、异步传输模式 ATM、因特网接入、电话网络中无线中继和帧中继等。CPS 是 MAC 的核心部分，主要功能包括系统接入、带宽分配、连接建立和连接维护等。PS 层提供基站和用户站之间的保密性，它包括两个部分：一是加密封装协议，负责空中传输的分组数据的加密；二是密钥管理协议，负责基站到用户站之间密钥的安全发放。

WiMAX(Worldwide interoperability for Microwave Access)即全球微波接入互操作性。WiMAX 系统主要有两个技术标准，一个是指满足固定宽带无线接入的 WiMAX 802.16d 标准；另一个是满足固定和移动的宽带无线接入技术 WiMAX 802.16e 标准。

无线城域网 WiMAX/802.16 参考模型如图 5-5 所示。

从图 5-5 中可知，WiMAX/IEEE 802.16 系统包括两个平面，数据/控制平面与管理平

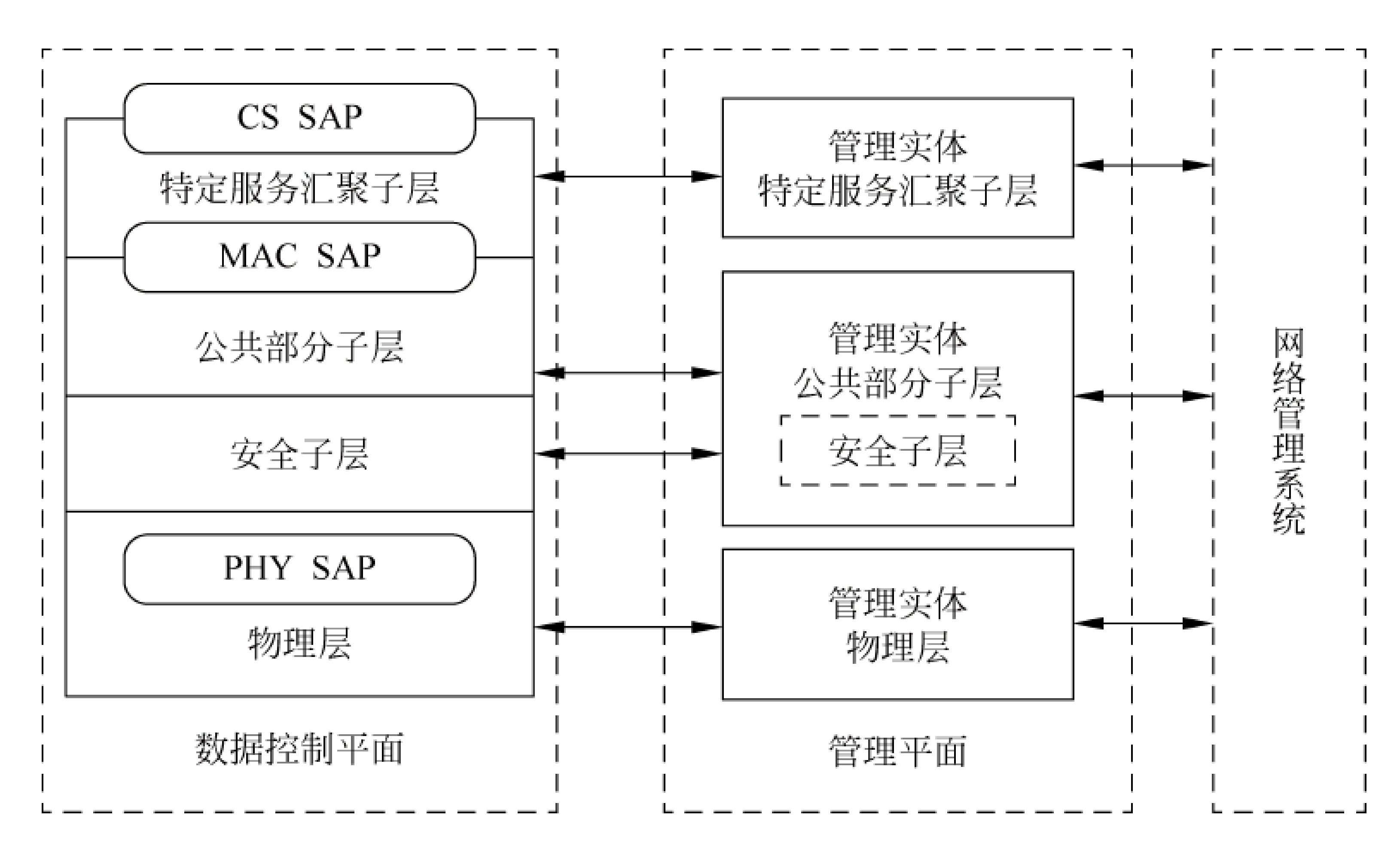


图 5-5 IEEE 802.16 参考模型

面。系统在数据/控制平面实现的功能主要是保证数据的正确传输。因此,数据/控制平面在定义了必要的传输功能之外,还需要定义一些控制机制来保障传输的顺利进行。而管理平面中定义的管理实体,分别与数据/控制平面的功能实体相对应,通过与数据/控制平面中实体的交互,管理实体可以协助外部的网络管理系统完成有关的管理功能。下面主要讨论WiMAX/802.16 系统的数据/控制平面。

WiMAX/802.16 标准为无线空中接口分别定义了介质访问控制(MAC)层和物理层。其中 MAC 层又可以划分为 3 个子层,分别是:面向业务的汇聚子层(CS),公共部分子层和安全子层。如图 5-5 所示,面向业务的汇聚子层通过业务汇聚服务访问点向上面的外部网络提供数据服务。而公共部分子层则通过 MAC 服务访问点为面向业务的汇聚子层提供服务。注意,公共部分子层和安全子层之间并不存在服务访问点,这是因为安全子层只是借助一套完整的加密算法来对需要发送的数据进行加密,并不存在提供某种服务的概念。

5.2.3 蓝牙网络安全

1. 蓝牙技术概述

蓝牙(Bluetooth)是一种支持设备短距离通信(通常为 10 米内)的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用“蓝牙”技术,能够有效地简化移动通信终端设备之间的通信,也能够成功地简化设备与因特网 Internet 之间的通信,从而数据传输变得更加迅速高效,为无线通信拓宽道路。

蓝牙采用分散式网络结构以及快跳频和短包技术,支持点对点及点对多点通信,工作在全球通用的 2.4GHz ISM(即工业、科学、医学)频段,其数据速率为 1Mbps。采用时分双工传输方案实现数据传输。

2. 蓝牙技术的特点

蓝牙技术是一个开放性、短距离无线通信的标准,它可以用来在较短距离内取代多种有线电缆连接方案,通过统一的短距离无线链路在各种数字设备之间实现方便、快捷、灵活、安

全、低成本、小功耗的语音和数据通信。

为保证在复杂的无线环境中能够安全可靠地工作，蓝牙技术采用"跳频"和"快速确认"技术以确保链路稳定。理论上蓝牙技术所采用的"跳频"技术可达到每秒 1600 次，共有 78 个可用的信道。

蓝牙技术支持三种信号发射功率，分别为 1mW、2.5mW 和 100mW。标准中所制定的各种发射功率对应覆盖范围分别为 10m、20m 和 100m。但是，无线信道在传输过程中受到的影响因素较多，发射功率与覆盖范围之间的关系难以准确计算。此外，材料、墙壁和其他 2.4GHz 信号的干扰都可能影响蓝牙信号的覆盖范围。

蓝牙支持最大为 1Mbps 的数据流量。由于需要考虑跳频、纠错开销、协议开销、加密和其他的因素，因此有效净荷传输的流量大约为 700～800kbps，这对于以替代有线电缆为目标的蓝牙技术而言已经足够了。其他工作在 2.4GHz 的无线通信设备，例如 IEEE 802.11b 的 WLAN 也会对蓝牙设备的信号造成干扰。

蓝牙是一个开放性、低功耗、低成本、短距离的无线通信标准，采用 FM 调制方式以抑制干扰、防止信号衰减并降低设备的复杂性；同时，蓝牙以时分双工(TDD)方式进行通信，其基带协议是电路交换和分组交换的组合。单个跳频频率发送一个同步分组，每个分组可以占用一个至五个时隙。蓝牙技术支持异步数据信道(ACL)，或者三个并发的语音信道(SCO)，并且也支持单个信道同时传送异步数据和同步语音。每一个语音信道支持 64kbps 同步语音；异步信道可以支持非对称连接，两个结点的数据速率发别为 721kbps 和 57.6kbps，也可以支持 432.6kbps 的对称连接。蓝牙采用前向纠错(FEC)编码技术，包括 1/3FEC、2/3FEC 和自动重传请求(ARQ)，以减少重发的次数，降低远距离传输时的随机噪声影响。然而，由于增加了冗余信息，增加了开销，使数据的流量减少。

蓝牙 4.0 是 2012 年最新发布的蓝牙版本，是 3.0 的升级版本；较 3.0 版本具有更省电、成本低、3 毫秒低延迟、超长有效连接距离、AES-128 加密等优点；通常用在蓝牙耳机、蓝牙音箱等移动设备上。

蓝牙 4.0 将三种技术规格集为一体，包括传统蓝牙技术、高速技术和低耗能技术，与 3.0 版本相比最大的不同就是低功耗。4.0 版本的功耗较老版本降低了 90%，比上一版本更省电。

随着蓝牙技术由手机、游戏、耳机、便携电脑和汽车等传统应用领域向物联网、医疗等新领域的扩展，对低功耗的要求会越来越高。4.0 版本强化了蓝牙在数据传输上的低功耗性能。

低功耗版本使蓝牙技术得以延伸到采用纽扣电池供电的一些新型产品中。蓝牙低耗能技术是基于蓝牙低耗能无线技术核心规格的升级版，为开拓物联网市场奠定了基础。

3. 蓝牙协议

蓝牙标准体系中的协议按特别兴趣小组 SIG 的关注程度分为四层：核心协议、串口仿真协议(RFCOMM)、电话控制协议(Telephone Control Protocol Specification，TCS)和选用协议。

核心协议包括基带(Base-Band，BB)协议、链路管理协议(Link Manager Protocol，LMP)、逻辑链路控制适配协议(Logic Link Control and Adaptation Protocol，L2CAP)、服

务发现协议(Service Discovery Protocol,SDP)。

选用协议包括点对点协议(Point to Point Protocol,PPP)、网际协议(IP)、传输控制协议(TCP)、用户数据报协议(User Datagram Protocol,UDP)、对象交换协议(OBEX)、无线应用协议(WAP)、电子名片(vCard)和电子日历(vCal)等。

除上述协议以外,蓝牙标准还定义了主机控制接口(Host Controller Interface,HCI),它为基带控制器、连接管理器、硬件状态和控制寄存器提供命令接口。

蓝牙核心协议由 SIG 制定的蓝牙专用协议组成,绝大部分蓝牙设备都需要核心协议,而其他协议则根据应用的需要而定。电缆替代协议、电话控制协议和被采用的协议在核心协议的基础上构成面向应用的协议。

4. 蓝牙网络的拓扑结构

蓝牙网络的拓扑结构如图 5-6 所示。蓝牙支持两种连接,即点对点和点对多点连接,这样就形成了两种不同的网络拓扑结构:微微网(Piconet)和散射网络(Scatternet)。微微网中只有一个主端设备(Master),最多支持七个从端设备(Slave)与主端设备通信。主端设备以不同的跳频序列来识别从端设备,并与之通信。若干个微微网形成一个散射网络,蓝牙设备既可以作为一个微微网中的主端设备,也可以在另一个微微网中作为从端设备。

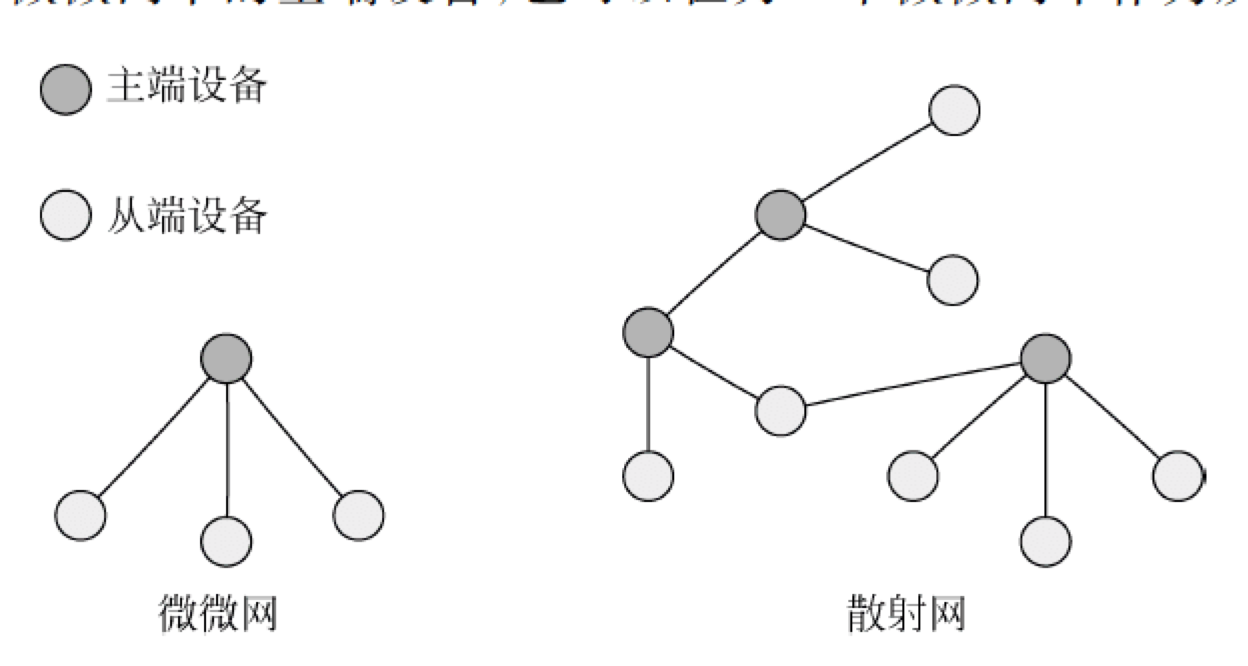


图 5-6 蓝牙网络的拓扑结构

多个微微网可以连接在一起,组成更大规模的网络,靠跳频顺序识别每一个微微网,同一个微微网的所有用户都与这个跳频顺序同步,其拓扑结构可以称为“多微微网”结构。在一个“多微微网”中,在带有 10 个全负载的独立微微网的情况下,全双工数据速率可超过 6M bps。

5. 蓝牙的工作原理

1) 蓝牙通信的主从关系

蓝牙技术规定每一对设备之间进行蓝牙通信时,必须一个为主端设备,另一个为从端设备,才能进行通信。通信刚开始时,必须由主端设备发起配对呼叫请求,通信链路建立成功后,双方即可收发数据。理论上,一个蓝牙主端设备,可同时与 7 个蓝牙从端设备进行通信。一个具备蓝牙通信功能的设备,可以在两个角色间切换,平时工作在从模式,等待其他主设备来连接,需要时,转换为主模式,向其他设备发起呼叫。一个蓝牙设备以主模式发起呼叫时,需要知道对方的蓝牙地址和配对密码等信息,配对完成后,可直接发起呼叫。

2）蓝牙的呼叫过程

蓝牙主端设备发起呼叫，首先是查找，找出周围处于可被查找的蓝牙设备。主端设备找到从端蓝牙设备后，与从端蓝牙设备进行配对，此时需要输入从端设备的 PIN 码，也有些设备不需要输入 PIN 码。配对完成后，从端蓝牙设备会记录主端设备的信任信息，此时主端即可向从端设备发起呼叫，已配对的设备在下次呼叫时，不再需要重新配对。已配对的设备，作为从端的蓝牙设备也可以发起建链请求，但用于数据通信的蓝牙模块一般不发起呼叫。链路建立成功后，主从两端之间即可进行双向的数据或语音通信。在通信状态下，主端和从端设备都可以发起断链请求，断开蓝牙链路。

6. 蓝牙安全分析

1）蓝牙技术的安全隐患

蓝牙采用了在 2.4GHz 频段上进行跳频扩展的工作模式，这种模式本身具有一定的通信隐蔽性。扩频通信可以允许比常规无线通信低得多的信噪比，并且蓝牙定义为近距离使用，因此其发射功率可以低至 1mW，这在一定程度上减少了其无线电波的辐射范围，增加了信息的隐蔽性。然而，从更为严格的安全角度来分析，物理信道上的这些基本的安全措施对于保证用户的信息安全是并不够的。在基于蓝牙技术的物联网应用中，其安全风险不容忽视。蓝牙技术主要的安全风险如下。

（1）蓝牙采用 ISM 2.4GHz 的频段收发无线电信号，这与许多同类通信协议产生冲突，例如 802.11b/802.11a/802.11n 等，容易对蓝牙通信产生干扰，使通信失效；

（2）无线电信号在传送过程中容易被截取、分析，失去信息的保密性；

（3）通信对端设备身份容易被冒充，使通信失去可靠性。

针对以上安全风险，在蓝牙系统中采用跳频扩展技术（Frequency-Hopping Spread Spectrum，FHSS），使蓝牙通信能够抵抗同类电磁波的干扰；并采用了加密技术来提高数据的保密性；采用身份鉴别机制来确保通信实体之间的可靠数据传输。虽然蓝牙系统所用的跳频技术已经提供了一定的安全措施，但是用蓝牙设备组建物联网时仍需要对网络层和应用层进行安全管理，设置更为复杂的安全体系。

2）蓝牙的安全体系架构

蓝牙的安全体系架构可以实现对业务的选择性访问，蓝牙安全架构建立在 L2CAP 层之上，特别是 RFCOMM 层。其他协议层对蓝牙架构没有什么特别的处理，它们有自己的安全特征。蓝牙安全架构允许协议栈中的协议强化其安全策略。例如，L2CAP 层在无绳电话方面强化了蓝牙安全策略，RFCOMM 层则在拨号网络方面强化了蓝牙安全策略，OBEX 在文件传输和同步应用方面采用自己的安全策略。蓝牙安全架构提供了一个灵活的安全框架，此框架指出了何时涉及用户的操作，下层协议层需要哪些动作来支持所需的安全检查等。在蓝牙系统中，安全架构是建立在链路级安全特征之上的，蓝牙技术的安全体系架构如图 5-7 所示，其中虚线为注册过程，实线则为查询过程。

安全管理器是蓝牙安全架构中最重要的部分，负责存储与业务和设备安全相关的信息，响应来自协议或者应用程序的访问需求，连接到应用程序前加强鉴权和加密，初始化或者处理来自用户以及外部安全控制实体的输入，在设备级建立信任连接等。

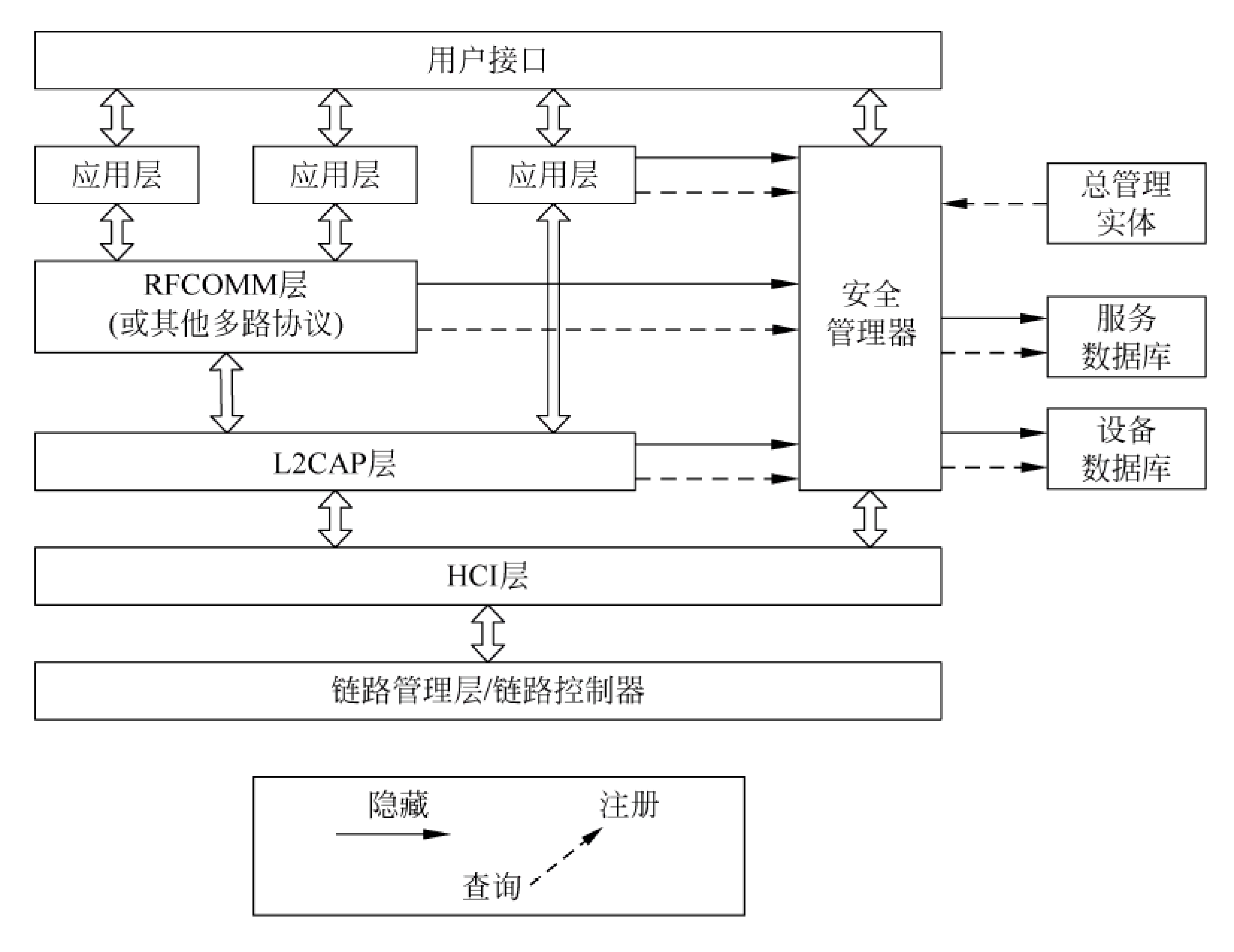


图 5-7 蓝牙的安全体系结构

7. 蓝牙的网络安全模式

蓝牙标准中定义了 3 种网络安全模式：非安全模式、强制业务级安全模式和强制链路级安全模式。

1) 非安全模式

在非安全模式中，蓝牙系统无任何安全需求，不需要任何安全服务和安全机制的保护，此时，任何设备和用户都可以任何类型的服务。在实际应用中，建议不要采用非安全模式。

2) 强制业务级安全模式

在强制业务级安全模式中，业务级安全机制对系统的各个应用和服务进行安全保护，包括授权访问、身份鉴别和加密传输。在这种模式下，加密和鉴别发生在逻辑链路控制和适配协议（Logical Link Controller and Adaptation Protocol，L2CAP）信道建立之前。

强制业务级安全模式中的安全管理器主要包括储存安全性信息、应答请求、强制鉴别和加密等关键任务。设备的 3 个信任等级和 3 种服务级别，分别存储在设备数据表和业务数据表中，并且由安全管理器维护。

每一个业务通过业务安全策略库和设备库来确定其安全等级。这两个库规定了：

(1) 甲设备访问乙设备是否需要授权；

(2) 甲设备访问乙设备是否需要身份鉴别；

(3) 甲设备访问乙设备是否需要数据加密传输。

强制业务级安全模式规定了何时需要和用户交互，以及为了满足特定的安全需求，协议层之间必须进行的安全行为。

安全管理器是这个安全体系结构的核心部分，它主要完成以下几项任务：

(1) 存储和查询有关服务的相关安全信息；

(2) 存储和查询有关设备的相关安全信息；

(3) 对应用、复用协议和 L2CAP 协议的访问请求(查询)进行响应；

(4) 在允许与应用建立连接之前，实施身份鉴别、数据加密等安全措施；

(5) 接收并处理 GME 的输入，以在设备级建立安全关系；

(6) 通过用户接口接收并处理用户或应用的个人识别码(Personal Identification Number，PIN)，以完成身份鉴别和加密。

强制业务级安全模式能定义设备和业务的安全等级。蓝牙设备可以分为可信任设备、不可信任设备和未知设备 3 种级别。可信任设备可以无限制地访问所有服务；不可信任设备访问业务受到限制；而未知设备视为不可信任设备，其访问业务同样受到限制。

在强制业务级安全模式中，蓝牙业务的安全级别主要由以下 3 个方面来保证：

(1) 授权要求：在授权之后，访问权限只自动赋给可信任设备，其他设备需要手工授权才能访问；

(2) 鉴别要求：在连接到一个应用之前，远程设备必须被鉴别；

(3) 加密要求：在访问业务发生之前，连接必须切换到加密模式。

对于设备和业务的访问权限取决于安全级别，各种业务可以事先注册，对于这些业务访问的级别取决于业务本身的安全机制。

3) 强制链路级安全模式

在强制链路级安全模式中，链路级安全机制对所有的应用和业务都需要实行访问授权、身份鉴别和加密传输。这种模式是强制业务层安全模式的极端情况，可以通过配置安全管理器并清除模块存储器中的链路密钥来达到目的，在强制链路级安全模式下，身份鉴别和加密发生在链路建立之前。

强制链路级安全模式与强制业务级安全模式之间的本质区别在于：在强制业务级安全模式下，蓝牙设备在信道建立之后启动安全性过程，即在较高层的协议上完成安全性过程；而在强制链路级安全模式下，蓝牙设备则是在信道建立之前启动安全性过程，即在低层协议上完成安全性过程。

蓝牙系统在链路层使用 4 种不同的信息安全单元来保证链路的安全：蓝牙单元独立地址(BD_ADDR)、业务处理随机数(RAND)、链路密钥、加密密钥。各信息安全单元的长度如表 5-1 所示。

表 5-1　蓝牙验证和加密过程中的信息安全单元

参　　数	长度(bit)
BD_ADDR	48
RAND	128
链路密钥	128
加密密钥	8～128

每一个蓝牙设备都有一个唯一的蓝牙单元独立地址(BD_ADDR)，它是一个 48bit 的 IEEE 地址，没有安全保护；业务处理随机数(RAND)也称为会话密钥，由蓝牙系统随机地生成；链路密钥和加密密钥在初始化时生成，它们是不公开的，加密密钥的长度可根据需求配置。

蓝牙的链路层安全模式是通过匹配、鉴权和加密实现的。密钥的建立是通过双向的链接来完成的；而鉴权和加密既可以在物理链接中实现，也可以通过上层的协议来实现。

（1）匹配。

两台蓝牙设备试图建立链接时，个人识别码（PIN）与一个随机数经必要的信息交换和计算创建初始密钥（K_{init}），此过程称为匹配。初始密钥在校验器向申请者发出随机数时创建。

（2）鉴权。

鉴权是蓝牙设备必须支持的安全特性，它是一个基于"挑战-应答"的方案，在这个方案中，申请者对于链路密钥和加密密钥，使用会话密钥经 2-MOV 协议进行验证。会话密钥指当前申请者/校验器共享的同一密钥，校验器将挑战申请者鉴权随机数输入，该输入含有鉴权码的 AU_RAND 标注，而该鉴权码则以 E_1 标注，申请者向校验器返回结果 SRES，蓝牙鉴权过程的工作原理如图 5-8 所示。

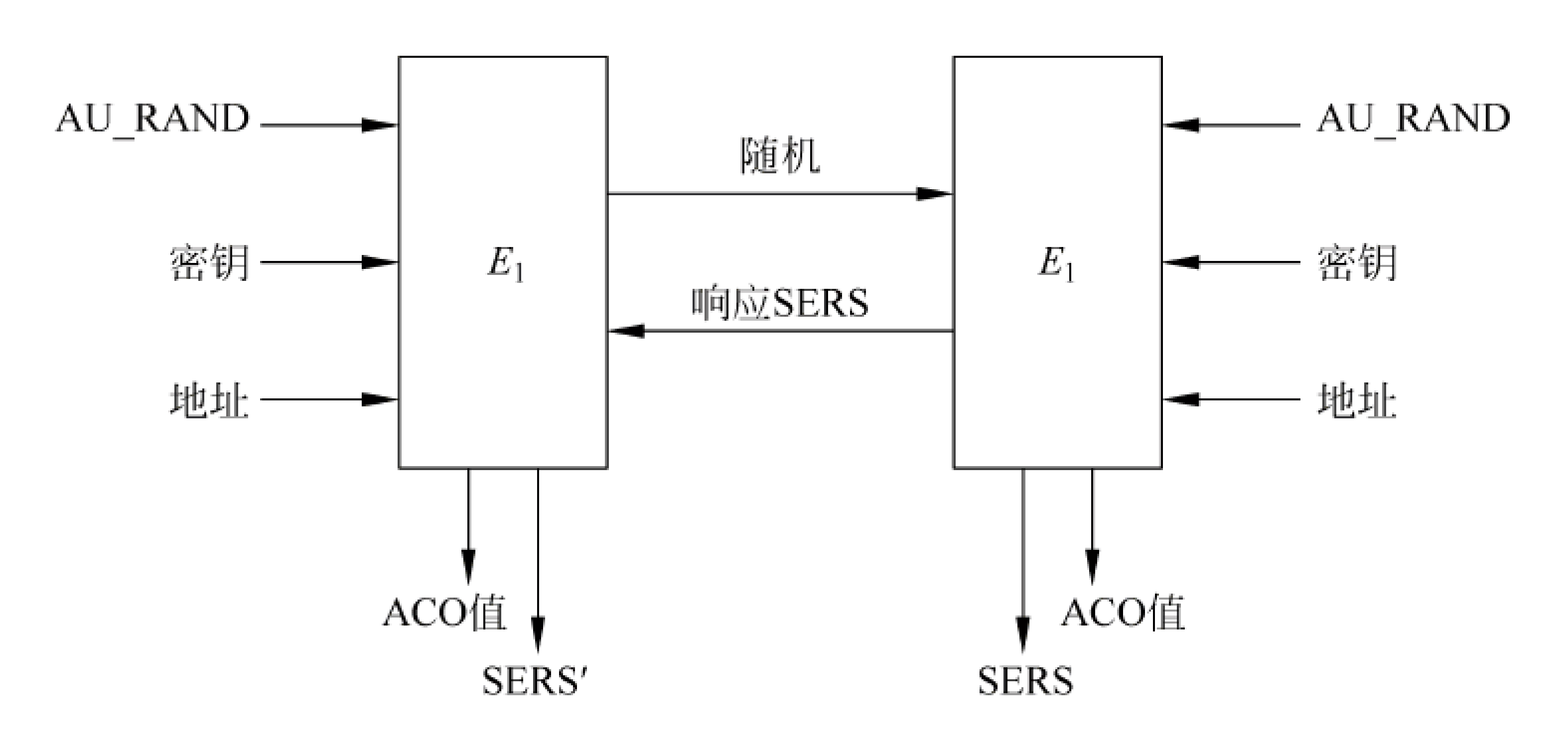


图 5-8　蓝牙的鉴权过程

在蓝牙系统中，校验器可以是主端设备，也可以是从端设备，既可以实施单向鉴权，也可以实施双向鉴权。

（3）加密。

蓝牙技术采用分组方式保护有效数据。对分组报头和其他控制信息不加密。用序列密码 E_0 对有效载荷加密，E_0 对每一个有效荷载重新同步。蓝牙的加密过程如图 5-9 所示。

加密过程由 3 个部分组成。第一部分设备初始化，同时生成加密密钥 K_C，具体计算由蓝牙 E_3 算法执行；第二部分由 E_0 计算出加密有效荷载的密钥；第三部分用 E_0 生成比特流，对有效荷载进行加密，解密过程则以同样的方式进行。

8. 蓝牙的密钥管理

蓝牙安全体系中主要使用 3 种密钥以确保安全的数据传输：个人识别码（PIN）、链路密钥和加密密钥。其中最重要的是链路密钥，用于两个蓝牙设备之间的相互鉴别。

1）个人识别码

个人识别码（Personal Identification Number，PIN）是一个由用户选择或固定的数字，长度可以为 1～16 个字节，通常为 4 位十进制数。用户在需要时可以改变个人识别码，以增加系统的安全性。在两个设备分别输入个人识别码比在其中一个使用固定的个人识别码要

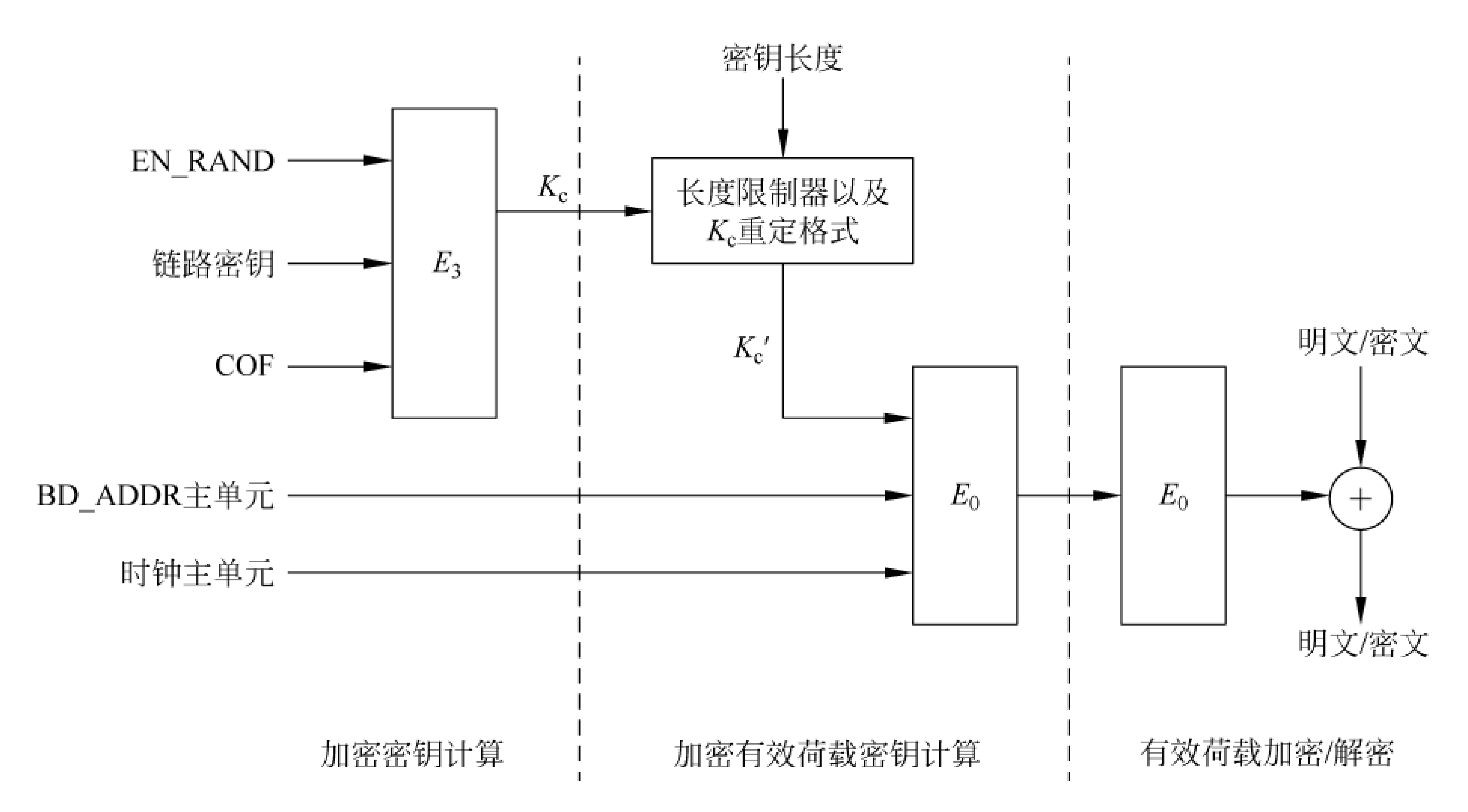


图 5-9　蓝牙的加密与解密过程

安全得多。

2）链路密钥

为满足不同的蓝牙应用需要，有 4 种不同的链路密钥。这 4 种链路密钥都是 128 位的随机数，它们分别是：

（1）单元密钥 K_A：K_A 在蓝牙设备安装时由单元 A 产生。它的存储只需要很少的内存单元，经常用于蓝牙设备只有少量内存或此蓝牙设备可被一个大的用户组访问的场合。

（2）联合密钥 K_{AB}：K_{AB}由单元 A 和单元 B 产生。每一对设备有各自的联合密钥，在需要更高的安全性时使用。

（3）主密钥 K_{master}：这种密钥在主设备需要同时向多个从设备传输数据时使用，在本次会话过程中它将临时替代原来的链路密钥。

（4）初始化密钥 K_{init}：在初始化过程中使用，用于保护初始化参数的传输。

3）加密密钥

加密密钥由当前的链路密钥推算而来。每次需要加密密钥时它会自动更换。将加密密钥与鉴权密钥分离开的原因是可以使用较短的加密密钥而不减弱鉴权过程的安全性。

4）密钥的生成与初始化

密钥的交换发生在初始化过程中，在两个需要进行鉴权和加密的设备上分别完成。初始化过程包括以下步骤：

（1）生成初始化密钥。

（2）鉴权。

（3）生成链路密钥。

（4）交换链路密钥。

（5）两个设备各自生成加密密钥。

在这些过程之后，链路或者建立成功或者建立失败。

5.2.4 ZigBee 网络安全

ZigBee 技术是一种可以实现短距离无线通信的新兴技术，它以功耗低、成本低、复杂程度低优胜于其他的短距离无线通信技术。ZigBee 这一名称（又称为紫蜂协议）来源于蜜蜂的八字舞，由于蜜蜂（bee）是靠飞翔和“嗡嗡”（Zig）地抖动翅膀的“舞蹈”来与同伴传递花粉所在方位信息，也就是说蜜蜂依靠这样的方式构成了群体中的通信网络。

ZigBee 技术以往称为 HomeRFLite、RF-Easylink 或 FireFly，如今统一称为 ZigBee。ZigBee 是一种类似于蓝牙技术和 RFID 技术的无线通信技术，主要应用于短距离内对传输速度要求不高的电子通信设备之间的数据传输，以及典型的、有周期性的、间歇性反应时间的数据传输。

ZigBee 技术作为短距离无线传感器网络的通信标准，可以广泛应用于家庭居住控制、商业建筑自动化和企业生产管理等领域。ZigBee 技术标准由 ZigBee 技术联盟于 2004 年推出，该联盟是一个由半导体厂商、技术供应商和原始设备制造商结盟的组织。由于具有低功耗、低延时、较长电池寿命等优点，使得它在低速率无线传感器网络中扮演着非常重要的角色，市场前景非常广阔。

1. ZigBee 技术的主要特点

ZigBee 技术相对于其他的无线通信技术，具有功耗低、成本较低、较短的传输范围、时延短、网络容量大、数据传输可靠性较高以及安全性高等主要特点。

1）功耗低

功耗低是 ZigBee 技术的一个主要特点。由于 ZigBee 的传输率低，传输数据量很少，并且采用了休眠模式，因此 ZigBee 设备非常省电。据估计，ZigBee 设备仅靠两节电池就可以维持长达六个月到两年时间所需要的电能。

2）成本较低

ZigBee 技术成本较低，原因是其协议简单，因而所需的内存空间小。ZigBee 不仅协议是免专利费的，而且芯片价格低，每块芯片只需要两美元。

3）较短的传输范围

一般来说，ZigBee 技术的室内传输距离在几十米以内，室外传输距离在几百米以内，属于近距离传输技术。

4）时延短

ZigBee 技术从休眠状态转入工作状态只需要 15ms，搜索设备时延为 30ms，活动设备信道接入时延为 15ms。作为比较，蓝牙技术时延需要 3～10s，Wi-Fi 则需要 3s。

5）网络容量大

ZigBee 的结点编址为两个字节，其网络结点容量理论上可达 65 535。

6）数据传输时的可靠性较高

ZigBee 技术中避免碰撞的机制通过为宽带预留时隙，可以避免传输数据时发生竞争和冲突。并且，通过 ZigBee 技术发送的每个数据包是否被对方接收都必须得到完全的确认，这就使得 ZigBee 技术在数据传输环节中具有较高的可靠性。

7）安全性高

ZigBee 提供了基于循环冗余校验的数据包完整性检查机制，支持鉴权和认证，采用 AES-128 高级加密算法，从而保护数据荷载和防止攻击者冒充合法设备。

2. ZigBee 安全技术分析

ZigBee 是针对低速率无线个人局域网，基于 IEEE 802.15.4 介质访问控制层和物理层标准，并在其基础上开发的一组包含组网、安全和应用软件方面的技术标准。在国际上，主要由 IEEE 802.15.4 小组和 ZigBee 联盟这两个组织负责 ZigBee 标准规范的制定。ZigBee 建立在 IEEE 802.15.4 标准之上，它确定了可在不同制造商之间共享的应用纲要。IEEE 802.15.4 仅定义了物理层和数据链路层。ZigBee 协议栈安全体系结构如图 5-10 所示。

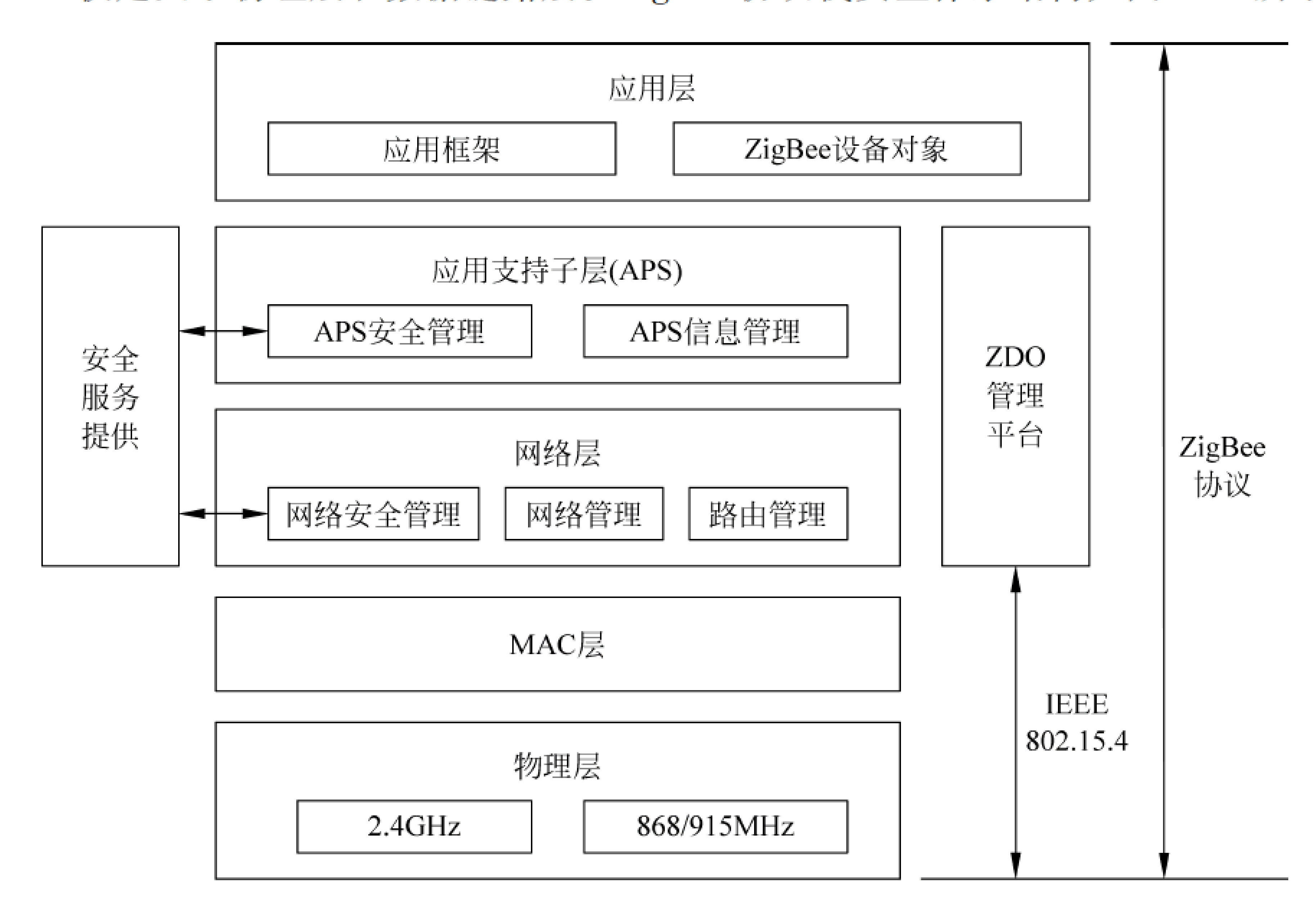


图 5-10　ZigBee 协议栈安全体系结构

1）物理层

ZigBee 兼容的产品工作在 IEEE 802.15.4 的物理层之上，可以工作在全球通用标准的 2.4GHz、美国标准的 915MHz 和欧洲标准的 868MHz 三个的频段上，并且在这三个频段上分别具有 250kbps、40kbps 和 20kbps 的最高数据传输速率。当使用 2.4GHz 频段时，ZigBee 技术室内传输距离为 10m，室外传输距离则能达到 200m；当使用其他频段，室内传输距离为 30m，室外传输距离则能达到 1000m。实际传输中，其传输距离根据发射功率确定，可以变化调整。

由于 ZigBee 使用的是开放频段，而这些频段已经使用了多种无线通信技术，因此为了避免互相干扰，各个频段均采用直接序列扩频技术。物理层的直接序列扩频技术允许设备无须闭环同步，在三个不同频段都采用相位调制技术。在 2.4GHz 频段采用较高阶的 QPSK 调制技术，以达到 250kbps 的速率，并降低工作时间，减少功率消耗。在 868MHz 和 915MHz 频段则采用 BPSK 的调制技术。与 2.4GHz 频段相比，868MHz 和 915MHz 频段

为低频频段，无线传输的损耗较少，传输距离较远。

2）数据链路层

IEEE 802 系列标准将数据链路层分为逻辑链路控制层（LLC）和介质接入控制层（MAC）两个子层。逻辑链路控制层负责传输的可靠性保障和控制、数据包的分段与重组、数据包的顺序传输工作，为 802 标准系列所共用。而介质接入控制层子层的协议则依赖于各自的物理层。IEEE 802.15.4 的 MAC 层能支持多种逻辑链路控制层标准，通过业务相关的汇聚子层协议承载。ZigBee 数据链路层安全帧结构如图 5-11 所示。

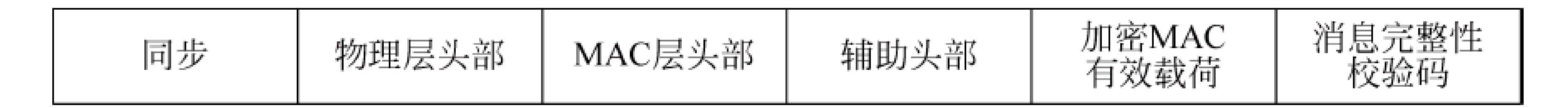


图 5-11　ZigBee 数据链路层安全帧结构

其中，辅助头部（Auxiliary Header，AH）携带安全信息，消息完整性校验码（MIC）提供数据完整性保护检查，其长度有 0、32、64、128 位可供选择。对于数据帧，MAC 层只能保证单跳通信安全，为了提供多跳通信的安全保障，必须依靠上层提供的安全服务。

IEEE 802.15.4 的 MAC 协议包括以下功能：设备之间无线链路的建立、维护和结束；确认模式的帧传输与接收；信道接入控制；帧校验；预留时隙管理；广播信息管理等。同时，使用 CSMA-CA 机制和应答重传机制，实现了信道的共享及数据帧的可靠传输。

3）网络层

网络层的主要功能是负责拓扑结构的建立和网络连接的维护，包括设计连接和断开网络时所采用的机制、帧传输过程中所采用的安全性机制、设备的路由发现和转交机制等。

ZigBee 网络层对帧采取的保护机制与数据链路层相同，为了保证帧能够正确传输，帧格式中也加入了辅助头部（AH）和消息完整性校验码（MIC）。网络层安全帧结构如图 5-12 所示。

同步	物理层头部	MAC层头部	网络层头部	辅助头部	加密MAC有效载荷	消息完整性校验码

图 5-12　ZigBee 网络层安全帧结构

网络层的主要思想是首先广播路由信息，接着处理接收到的路由信息，如判断数据帧来源，然后根据数据帧中的目的地址采取相应机制将数据帧传送出去。在传送的过程中通常是利用链接密钥对数据进行加密处理，如果链接密钥不可用，则网络层将利用网络密钥进行保护。由于网络密钥在多个设备中使用，可能带来内部攻击，但是它的存储开销更小。在管理方面，网络层主要实现网络安全管理、网络管理和路由管理。

4）应用层

应用层主要负责把不同的应用映射到 ZigBee 网络，主要包括三部分：与网络层连接的应用支持子层（Application Support Sublayer，APS）、ZigBee 设备对象（ZigBee Device Obiect，ZDO）和 ZigBee 的应用层框架（Application Framework，AF）。

应用支持子层（APS）提供了两个接口，分别是应用支持子层数据实体服务访问点（APSDE-SAP）和应用支持子层管理实体服务访问点（APSME-SAP）。同时，应用支持子层的接口是从应用商定义的应用对象到 ZDO 之间的服务集。应用支持子层数据实体提供的

数据通信是在相同的网络中,在一个或者多个应用实体之间的。APS 管理实体提供的主要是维护数据库的服务,也有绑定设备等服务。

ZigBee 应用层安全是通过应用支持子层(APS)提供的,根据不同的应用需求采用不同的密钥,主要使用链接密钥和网络密钥。应用层安全帧格式如图 5-13 所示。

同步	物理层头部	MAC层头部	网络层头部	应用支持子层头部	辅助头部	加密MAC有效载荷	消息完整性校验码

图 5-13 ZigBee 应用层安全帧格式

APS 提供的安全服务有密钥建立、密钥传输、设备服务管理。密钥建立在两个设备之间进行,包括 4 个步骤:交换暂时数据、生成共享密钥、获得链接密钥和确认链接密钥。密钥传输服务是指设备之间安全传输密钥。设备服务管理包括更新设备和移除设备,更新设备服务提供一种安全的方式通知其他设备有第三方设备需要更新,移除设备则是通知有设备不符合安全需要,要被删除。

5.2.5 超宽带网络安全

超宽带(Ultra Wide Band,UWB)技术起源于 20 世纪 50 年代末,早期主要作为一种军用通信技术,在雷达探测和定位等军事领域中使用。2002 年 2 月,美国联邦通信委员会批准超宽带技术进入民用领域,普通用户不需要申请即可使用。

1. 超宽带技术的特点

作为一种重要的近距离通信技术,超宽带技术在需要传输宽带感知信息的物联网应用领域具有广阔的应用前景。与现有的无线通信技术相比,超宽带技术具有以下主要特点:

1) 低成本

UWB 产品不再需要复杂的射频转换电路和调制电路,它只需要一种数字方式来产生脉冲,并对脉冲进行数字调制,而这些电路都可以被集成到一个芯片上。因此,其收发电路的成本很低,在集成芯片上加上时钟电路和一个微控制器,就可以构成一个超宽带通信设备。

2) 传输速率高

为了确保提供高质量的多媒体业务的无线网络,其信息传输速率不能低于 50M bps。在民用产品中,一般要求 UWB 信号的传输范围在十米以内,再根据经过修改的信道容量公式,其传输速率可达 500M bps,是实现无线个域网的一种理想调制技术。UWB 以非常宽的频率来换取高速的数据传输,并且不单独占用现在的频率资源,而是共享其他无线技术使用的频带。

3) 空间容量大

UWB 无线通信技术的单位区域内通信容量可以超过每平方米 1000kbps,而 IEEE 802.11b 仅为每平方米 1kbps,蓝牙技术为每平方米 30kbps,IEEE 802.11a 也只有每平方米 83kbps。由此可见,目前常用的无线技术标准的空间容量都远低于 UWB 技术。随着技术的不断完善,UWB 系统的通信速率、传输距离及空间容量还将不断提高。

4) 低功耗

UWB 使用简单的传输方式发出的是瞬间尖波形电波,即所谓的脉冲电波,它直接发送

0 或 1 脉冲信号出去，脉冲持续时间很短，仅为 0.2～1.5 纳秒，由于只在需要时发送脉冲电波，因此 UWB 系统的功耗很低，仅为 1～4mW，民用的 UWB 设备功率一般是传统移动电话或者无线局域网所需功率的十分之一到一百分之一左右，大大延长了电源的供电时间。UWB 设备在电池寿命和电池辐射上相对于传统无线设备有着很大的优越性。

2. 超宽带面临的信息安全威胁

由于超宽带网络的独特特征，使得网络非常脆弱，很容易受到各种安全威胁和攻击。而传统加密和安全认证机制等安全技术，虽然能够在一定程度上避免 UWB 网络中的入侵，但是面临的信息安全形势仍然严峻。超宽带面临的信息安全威胁如下：

1）拒绝服务攻击

拒绝服务攻击是使结点无法对其他合法结点提供所需正常服务的攻击。在无线通信中，攻击者的攻击目标可以是任意的移动接点，并且攻击可以来自各个方向，拒绝服务攻击可以发生在 UWB 网络中的各个层。在物理层和媒体接入层，攻击者通过无线干扰来拥塞通信信道；在网络层，攻击者可以破坏路由信息，使得网络无法互联；在更高层，攻击者可以攻击各种高层服务。拒绝服务攻击的后果取决于 UWB 网络的应用环境，在 UWB 网络中，使中心资源溢出的拒绝服务攻击威胁甚少，UWB 网络各个结点相互依赖的特点，使分布式的拒绝服务攻击威胁更为严重。如果攻击者有足够的计算能力和运行带宽，较小的 UWB 网络可能非常容易阻塞，甚至崩溃。在 UWB 网络中，剥夺睡眠攻击是一种特殊的拒绝服务攻击，攻击者不停地通过合法方式与结点交互，其目的就是消耗结点的有限的电池能量，使结点无法正常工作。

2）密钥泄露

在传统公钥密码体制中，用户采用加密、数字签名等技术来实现信息的机密性和完整性等安全服务。但这需要一个信任的认证中心，而 UWB 网络不允许存在单一的认证中心，否则单一的认证中心崩溃将造成整个网络无法获得认证，而且被攻破的认证中心的私钥可能会泄露给攻击者，使得整个网络完全失去安全性。

3）假冒攻击

假冒攻击在超宽带网络的各个层次都可以进行。它可以威胁到 UWB 网络结构的所有层。如果没有适当的身份认证，恶意结点就可以伪装成其他信任的结点，从而破坏整个网络的正常运行。例如，Sybil 攻击就是这样一种攻击。如果没有适当用户验证的支持，在网络层，泄密结点就可以冒充其他被信任结点攻击网络而不会暴露。例如，加入网络或者发送虚假的路由信息；在网络管理范围内，攻击者可以作为超级用户获得对配置系统的访问；在服务层，一个恶意用户甚至不需要适当的证书就可以拥有经过授权的公钥。成功的假冒攻击所造成的结果非常严重。一个恶意用户可以假冒任何一个友好结点，向其他结点发布虚假的命令和状态信息，并对其他结点或服务造成永久性的毁坏。同时 UWB 网络的这些安全缺陷也导致在传统网络中能够较好工作的安全机制，如加密和认证机制、防火墙以及网络安全方案，不能够有效地适用于 UWB 网络。

4）路由攻击

路由攻击包括内部攻击和外部攻击。内部攻击源于网络内部，这种攻击对路由信息将造成很大的威胁。外部攻击中除了常规的路由表溢出攻击等外部攻击以外，还包括隧道攻

击、睡眠剥夺攻击和结点自私性攻击等针对移动自组网的独特攻击。

3. 超宽带技术的安全规范

与传统的有线网络相比，无线网络的安全问题往往是出乎预料的，由于分布式无线网络各种各样的应用，使其安全问题更加复杂。

1）安全性要求

针对超宽带网络应用过程中容易发生的信息安全问题，国际标准化组织接受了由WiMedia联盟提出的《高速率超宽带通信的物理层和媒体接入控制标准》，即ECMA-368（ISO/IEC26907），它规范了相应的安全性要求。

（1）安全级别。

ECMA-368（ISO/IEC26907）标准定义了两种安全级别：无完全和强安全保护。安全保护包括数据加密、消息认证和重播攻击防护；安全帧提供对数据帧、选择帧和控制帧的保护。

（2）安全模式。

安全模式指一个设备是否被允许建立与其他设备进行数据通信的安全关系。ECMA-368（ISO/IEC26907）标准定义了三种安全模式，用于控制设备间的通信。两台设备通过四次握手协议来建立安全关系。一旦两台设备建立了安全关系，它们将使用安全帧来作为数据帧，如果接收方需要接受安全帧，而发送方无安全帧，那么接收方将丢弃该帧。

安全模式0定义了数据传输时使用无安全帧的通信方式，并且与其他设备建立无安全关系的通信方式。在该模式下，如果接收到安全帧，MAC层将直接丢弃该帧。

安全模式1定义了数据传输时与安全模式0下的设备进行数据通信，或者未建立安全关系的处于安全模式1下的设备进行数据通信，或者在特定帧的控制下与处于安全模式1下建立安全关系的设备进行通信；否则将丢弃数据帧。

安全模式2的安全级别比较高，它不与其他安全模式的设备进行通信，而是通过四次握手协议建立安全关系。

（3）握手协议。

四次握手协议使得两台具有共享主密钥的设备进行相互认证，同时产生PTK（Pairwise Transient Key）来加密特定的帧。

（4）密钥传输。

在成功地四次握手并建立安全关系后，两台设备开始分发各自的GTK（Group Transient Key）。GTK用于组播通信时对传输数据的加密。每个GTK的分发是通过四次握手中产生的PTK进行加密后再进行传送的。

2）信息接收与验证

在信息接收过程中，接收帧时，MAC子层的信息处理流程如图5-14所示。

帧重发机制保护接收方有效地接收FCS和MIC安全帧，其信息接收流程为：从接收帧中提取出SFN，将其与此帧所用的临时密钥的重发计数器的值作比较。如果前者小于或等于后者，接收方的MAC子层丢弃此帧；否则，接收方将接收到的SFN赋给相应的重发计数器。不过，使用此SFN更新重发计数器前，接收方应确保此帧已通过FCS验证、重发预防和MIC确认。

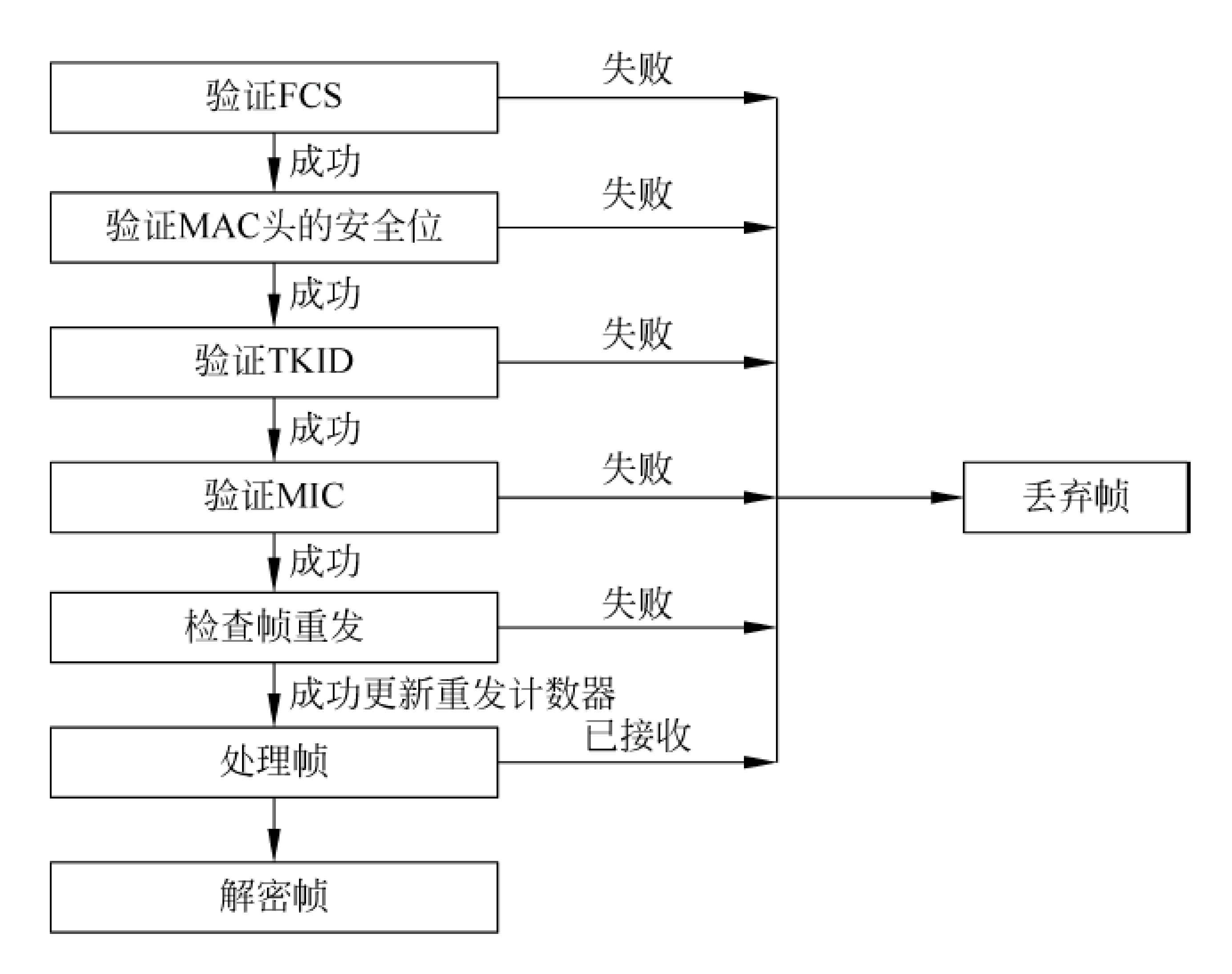


图 5-14　MAC 子层信息处理流程

3）MAC 层的信息安全传输机制

在超宽带系统中，MAC 层的信息安全传输功能主要包括以下几个方面：

（1）通过物理层，在一个无线频道上与对等设备进行通信。

（2）采用基于动态配置的分布式信道访问方式。

（3）基于竞争的信道访问方式。

（4）采用同步的方式进行协调应用。

（5）提供在设备移动和干扰环境下的有效解决方案。

（6）以调度帧传送和接收的方式来控制设备功耗。

（7）提供安全的数据认证和加密方式。

（8）提供设备间距离计算方案。

超宽带的 MAC 层是一种完全分布式的结构，没有一台设备处于中心控制的角色。所有设备都具有上述 8 种功能，并且根据应用的不同可以选择性的使用这 8 种功能。在分布式环境中，设备间通过信标帧的交换来识别。设备的发现、网络结构的动态重组和设备移动性的支持，都是通过进行周期性的信标传输来实现的。

4. 超宽带拒绝服务攻击防御策略

以往，拒绝服务攻击主要是针对计算机网络系统的。随着通信技术的发展，目前拒绝服务攻击已经有针对所有通信系统的发展趋势。由于超宽带是一种开放的分布式网络，没有中央控制。因此，基于 UWB 的物联网在运营过程中受到拒绝服务攻击的可能性就大大提高了。

1）超宽带拒绝服务攻击的工作原理

超宽带拒绝服务攻击的工作原理如图 5-15 所示。

拒绝服务是指网络信息系统由于某种原因遭到不同程度的破坏，使得系统资源的可用性降低甚至不可用，从而导致不能为授权用户提供正常的服务。拒绝服务通常是由配置错

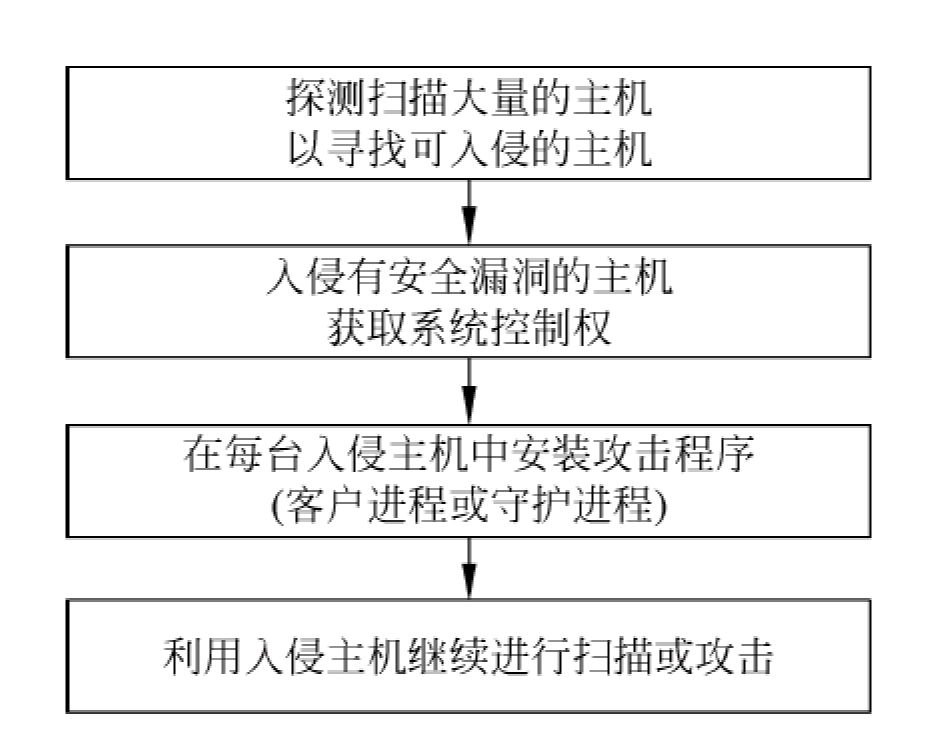


图 5-15 UWB 拒绝服务攻击流程

误、软件弱点、资源毁坏、资源耗尽和资源过载等因素引起的。其工作原理是利用工具软件，集中在某一时间段内向目标机发送大量的垃圾信息，或者是发送超过目标机接收能力的信息，使得对方出现网络堵塞或负载过重等状况，造成目标系统拒绝服务。在实际网络中，由于网络规模和速度的限制，攻击者往往难以在短时间内发送过多的请求，因此通常都采用分布式拒绝服务攻击的方式。在这种攻击中，为了提高攻击的成功率，攻击者需要控制大量的被入侵主机。因此攻击者一般会采用一些远程控制软件，以便在自己的客户端操纵整个攻击过程。

值得注意的是，在利用入侵主机继续进行扫描和攻击的过程中，采用分布式拒绝服务的客户端通常采用 IP 欺骗技术，以逃避追查。

2）超宽带网络中拒绝服务攻击的类型

在超宽带网络中，拒绝服务攻击主要有两种类型：MAC 层攻击和网络层攻击。

在 MAC 层实施的拒绝服务攻击主要有两种方法：一种方法是拥塞 UWB 网络中的目标结点设备使用的无线信道，使得 UWB 网络中的目标结点设备不可用；另一种方法是将 UWB 网络中的目标结点设备作为网桥，让其不停地中继转发无效的数据帧，以耗尽 UWB 网络中的目标结点设备的可用资源。

在网络层实施的攻击也称为 UWB 路由攻击，其主要攻击方法有以下四种：

（1）UWB 网络的多个结点通过与 UWB 网络中的被攻击目标结点设备，建立大量的无效的 TCP 连接来消耗目标结点设备的 TCP 资源，使得正常的连接不能进入，从而降低甚至耗尽系统的资源。

（2）UWB 网络的多个结点同时向 UWB 网络中的目标结点设备发送大量伪造的路由更新数据包，使得目标结点设备忙于频繁的无效路由更新，以此降低系统的性能。

（3）通过 IP 地址欺骗技术，攻击结点通过向路由器的广播地址发送虚假信息，使得路由器所在网络上的每台设备向 UWB 网络中的目标结点设备回复该信息，从而降低系统的性能。

（4）修改 IP 数据包头部的 TTL 域，使得数据包无法到达 UWB 网络中的目标结点设备。

3）超宽带网络中拒绝服务攻击的防御措施

针对 UWB 网络中基于数据报文的拒绝服务攻击，可以采用路由路径删除措施来防止

UWB 洪泛拒绝服务攻击。

当攻击者发动基于数据报文的 UWB 洪泛攻击行为时，发送大量攻击数据报文至所有 UWB 网络中的结点。作为邻居结点和沿途结点是难以判别攻击行为的，因为结点无法判断数据报文的用途。但作为数据报文的目标结点，就比较容易判定了。当目标结点发现收到的报文都是无用的时候，它就可以认定源结点为攻击者。目标结点可以通过路径删除的方法来阻止基于数据报文的 UWB 洪泛攻击行为。

具体的实施步骤是：当网络中的目标结点发现源结点是攻击者时，由目标结点生成一个路由请求报文（RRER），该报文标明目标结点不可达，目标结点将这个 RRER 报文发送给攻击者。当 RRER 报文到达攻击者时，它就会认为这条路由已经中断，从而将这条路由从本结点的路由表中删除，这样它就无法继续发送攻击报文了。假如它还要发送报文，就必须重新建立路由。这时，目标结点已经判定该结点为攻击者，对它发送的 RREQ 报文不回答 RREP，这样就无法重新建立路由。通过这种方式，只要被攻击过的结点都会拒绝攻击者建立路由。如果攻击者不断发动基于数据报文的 UWB 拒绝服务攻击，拒绝与其建立路由的结点就会越来越多，最后所有结点都会拒绝与其建立路由，攻击者就会被孤立于 UWB 网络之外，从而阻止了基于数据报文的 UWB 拒绝服务攻击。

随着物联网应用领域的不断发展，对于物联网末端感知信息的需求会不断增加，在物联网末端的信息感知网络中应用超宽带技术具有越来越重要的意义。目前对于超宽带应用过程中的信息安全机制虽然有一定的研究，但是仍然处于初级阶段，还需要针对物联网的运营环境和面临的新型信息安全威胁进行更为深入的研究，以满足物联网产业日新月异的发展需求。

5.3　移动通信系统安全

5.3.1　移动通信系统概述

到目前为止，移动通信系统的发展已经经历了四个时代，如图 5-16 所示。

时代	标准	技术	短信	语音	数据	数据传输
1G	AMPS, TACS	模拟	不支持	电路		无
2G	GSM,CDMA GPRS,EDGE	数字	支持	电路		9.6~384k
3G	WCDMA,CDMA2000 TD-SCDMA,HSPA			电路	分组	下行 2~42M
3.9G	LTE,WiMAX			分组		下行峰值 100M

图 5-16　移动通信系统的发展时代

1. 第一代移动通信系统

第一代移动通信系统简称为 1G，主要采用蜂窝组网和频分多址（FDMA）技术。由于受

到传输带宽的限制,不能进行移动通信的长途漫游,只能是一种区域性的移动通信系统。第一代移动通信有多种制式,我国主要采用的是 TACS。第一代移动通信有很多不足之处,如容量有限、制式太多、互不兼容、保密性差、通话质量不高、不能提供数据业务和不能提供自动漫游等。

回顾第一代移动通信系统,就不能不提起大名鼎鼎的美国贝尔实验室。1978 年底,贝尔实验室研制成功了全球第一个移动蜂窝电话系统——先进移动电话系统(Advanced Mobile Phone System,AMPS)。5 年后,这套系统在芝加哥正式投入商用并迅速在全美国推广,获得了巨大成功。

同一时期,欧洲各国也不甘示弱,先后建立起自己的第一代移动通信系统。瑞典等北欧 4 国合作,在 1980 年研制成功了 NMT-450 移动通信网并投入使用;联邦德国在 1984 年完成了 C 网络(C-Netz);英国则于 1985 年开发出频段在 900MHz 的全接入通信系统(Total Access Communications System,TACS)。

在各种 1G 系统中,美国 AMPS 制式的移动通信系统在全球的应用最为广泛,它曾经在超过 72 个国家和地区运营,直到 1997 年还在一些地方使用。同时,也有近 30 个国家和地区采用英国 TACS 制式的 1G 系统。这两种移动通信系统是世界上最具影响力的 1G 系统。

中国的第一代模拟移动通信系统,于 1987 年 11 月 18 日在广东第六届全运会上开通,并正式开始投入商用,采用的是英国 TACS 制式。从中国电信 1987 年 11 月开始运营模拟移动电话业务到 2001 年 12 月底中国移动关闭模拟移动通信网,1G 系统在中国的应用长达 14 年,用户数最高曾达到了 660 万。如今,1G 时代那像砖头一样的手持终端——大哥大,已经成为了很多人的美好回忆。

第一代移动通信系统的主要特点是采用频分复用技术,语音信号为模拟调制,每隔 30kHz/25kHz 一个模拟用户信道。第一代移动通信系统在商业上取得了巨大的成功,但是其缺点也日渐显露出来。

(1) 频谱利用率低。

(2) 业务种类有限。

(3) 无高速数据业务。

(4) 保密性差,易被窃听和盗号。

(5) 设备成本高。

(6) 体积大,重量大。

2. 第二代移动通信系统

为了解决模拟系统中存在的这些根本性技术缺陷,数字移动通信技术应运而生,并且逐渐发展起来,这就是第二代移动通信系统(简称 2G),时间是从 20 世纪 80 年代中期开始的。第二代移动通信系统以传输话音和低速数据业务为目的,因此又称为窄带数字通信系统。第二代数字蜂窝移动通信系统的典型代表是美国的 DAMPS 系统、IS-95 系统和欧洲的 GSM 系统。

(1) 先进的数字移动电话系统(DAMPS)也称 IS-54(北美数字蜂窝),使用 800MHz 频带,是两种北美数字蜂窝标准中推出较早的一种,指定使用 TDMA 多址方式。

(2) IS-95 是北美的另一种数字蜂窝标准,使用 800MHz 或 1900MHz 频带,使用

CDMA 多址方式，已成为美国个人通信系统(PCS)网的首选技术。

(3) 全球移动通信系统(GSM)发源于欧洲，它是作为全球数字蜂窝通信的 DMA 标准而设计的，支持 64kbps 的数据速率，可与 ISDN 互连。GSM 使用 900MHz 频带，使用 1800MHz 频带的称为 DCS1800。GSM 采用 FDD 双工方式和 TDMA 多址方式，每载频支持 8 个信道，信号带宽 200kHz。GSM 标准体制较为完善，技术相对成熟，不足之处是相对于模拟系统容量增加不多，仅仅为模拟系统的两倍左右，且无法和模拟系统兼容。

由于第二代移动通信以传输话音和低速数据业务为目的，从 1996 年开始，为了解决中速数据传输问题，又出现了 2.5 代的移动通信系统，如 GPRS 和 IS-95B。

3. 第三代移动通信系统

3G 即第三代移动通信技术，是指支持高速数据传输的蜂窝移动通信技术。3G 服务能够同时传送声音及数据信息，速率一般在几百“kbps”以上。3G 是指将无线通信与国际互联网等多媒体通信结合的新一代移动通信系统，目前 3G 存在 3 种标准：CDMA2000、WCDMA、TD-SCDMA。

3G 下行速度峰值理论可达 3.6Mbit/s，上行速度峰值也可达 384kbit/s。

中国大陆支持国际电联确定的三个无线接口标准，分别是中国电信的 CDMA2000，中国联通的 WCDMA，中国移动的 TD-SCDMA，GSM 设备采用的是时分多址，而 CDMA 使用码分扩频技术，先进功率和话音激活至少可提供大于 3 倍 GSM 网络容量，业界将 CDMA 技术作为 3G 的主流技术，国际电联确定三个无线接口标准，分别是美国 CDMA2000，欧洲 WCDMA，中国 TD-SCDMA。原中国联通的 CDMA 卖给中国电信，中国电信已经将 CDMA 升级到 3G 网络，3G 主要特征是可提供移动宽带多媒体业务。

已有 538 个 WCDMA 运营商在 246 个国家和地区开通了 WCDMA 网络，3G 商用市场份额超过 80%，而 WCDMA 向下兼容的 GSM 网络已覆盖 184 个国家，遍布全球，WCDMA 用户数已超过 6 亿。

1) WCDMA

WCDMA，全称为 Wideband CDMA，也称为 CDMA Direct Spread，意为宽频分码多重存取，这是基于 GSM 网发展出来的 3G 技术规范，是欧洲提出的宽带 CDMA 技术，它与日本提出的宽带 CDMA 技术基本相同，目前正在进一步融合。WCDMA 的支持者主要是以 GSM 系统为主的欧洲厂商，日本公司也或多或少参与其中，包括欧美的爱立信、阿尔卡特、诺基亚、朗讯、北电，以及日本的 NTT、富士通、夏普等厂商。该标准提出了 GSM(2G)-GPRS-EDGE-WCDMA(3G)的演进策略。这套系统能够架设在现有的 GSM 网络上，对于系统提供商而言可以较轻易地过渡。预计在 GSM 系统相当普及的亚洲，对这套新技术的接受度会相当高。因此 WCDMA 具有先天的市场优势。WCDMA 已是当前世界上采用的国家及地区最广泛的，终端种类最丰富的一种 3G 标准，占据全球 80%以上的市场份额。

2) CDMA2000

CDMA2000 是由窄带 CDMA(CDMA IS95)技术发展而来的宽带 CDMA 技术，也称为 CDMA Multi-Carrier，它最先由美国高通北美公司提出，摩托罗拉、Lucent 和后来加入的韩国三星都有参与，后来韩国三星成为该标准的主导者。这套系统是从窄频 CDMAOne 数字标准衍生出来的，可以从原有的 CDMAOne 结构直接升级到 3G，建设成本低廉。但使用

CDMA的地区只有日、韩和北美,所以CDMA2000的支持者不如WCDMA多。不过CDMA2000的研发技术却是目前各标准中进展最快的。该标准提出了从CDMAIS95(2G)-CDMA20001x-CDMA20003x(3G)的演进策略。CDMA20001x被称为2.5代移动通信技术。CDMA20003x与CDMA20001x的主要区别在于应用了多路载波技术,通过采用三载波使带宽提高。中国电信正在采用这一方案向3G过渡,并已建成了CDMAIS95网络。

3) TD-SCDMA

TD-SCDMA全称为Time Division-Synchronous CDMA(时分同步CDMA),该标准是由中国独自制定的3G标准。1999年6月29日,中国原邮电部电信科学技术研究院(大唐电信)向ITU提出该项技术,但技术发明始于西门子公司。TD-SCDMA具有辐射低的特点,被誉为绿色3G。该标准将智能无线、同步CDMA和软件无线电等当今国际领先技术融于其中,在频谱利用率、对业务支持具有灵活性、频率灵活性及成本等方面的独特优势。另外,由于中国内地庞大的市场,该标准受到各大主要电信设备厂商的重视,全球一半以上的设备厂商都宣布可以支持TD-SCDMA标准。该标准提出不经过2.5代的中间环节,直接向3G过渡,非常适用于GSM系统向3G升级。军用通信网也是TD-SCDMA的核心任务。相对于另外两个3G标准CDMA2000和WCDMA,它的起步较晚,技术不够成熟。

4. 第四代移动通信系统

第四代移动通信系统,英文缩写为4G。该技术包括TD-LTE和FDD-LTE两种制式。严格意义上来讲,LTE只是3.9G,尽管被宣传为4G无线标准,但它其实并未被3GPP认可为国际电信联盟所描述的下一代无线通信标准IMT-Advanced,因此在严格意义上其还未达到4G的标准。只有升级版的LTE Advanced才满足国际电信联盟对4G的要求。

4G技术集LTE技术与WiMAX技术于一体,并能够快速传输数据、高质量、音频、视频和图像等。4G能够以100Mbps的峰值速率下载,比目前的家用宽带ADSL(4兆)快25倍,并能够满足几乎所有用户对于无线服务的要求。此外,4G可以在DSL和有线电视调制解调器没有覆盖的地方部署,然后再扩展到整个地区。很明显,4G有着不可比拟的优越性。

长期演进(Long Term Evolution,LTE)项目是3G的演进,它改进并增强了3G的空中接入技术,采用OFDM和MIMO作为其无线网络演进的唯一标准。根据4G牌照发布的规定,国内三家运营商中国移动、中国电信和中国联通,都拿到了TD-LTE制式的4G牌照。

LTE主要特点是在20MHz频谱带宽下能够提供下行100Mbit/s与上行50Mbit/s的峰值速率,相对于3G网络大大地提高了小区的容量,同时将网络延迟大大降低。内部单向传输时延低于5ms,控制平面从睡眠状态到激活状态迁移时间低于50ms,从驻留状态到激活状态的迁移时间小于100ms。并且这一标准也是3GPP长期演进(LTE)项目,是近年来3GPP启动的最大的新技术研发项目。

WiMAX (Worldwide Interoperability for Microwave Access),即全球微波互联接入,本书的5.2.2章节已经详细地介绍过WiMAX,这里不再重复。

5.3.2 移动通信系统面临的安全威胁

移动通信系统面临的安全威胁来自网络协议和系统的弱点。攻击者可以利用网络协议和系统的弱点,非授权访问敏感数据、非授权处理敏感数据、干扰或滥用网络服务,对用户和

网络资源造成损失。

按照攻击的物理位置，对移动通信系统的安全威胁可分为对无线链路的威胁、对服务网络的威胁和对移动终端的威胁。主要威胁方式有以下几种：

1. 窃听

在无线链路或服务网内窃听用户数据、信令数据及控制数。

2. 伪装

伪装成网络单元截取用户数据、信令数据及控制数据，伪终端欺骗网络获取服务。

3. 流量分析

主动或被动进行流量分析以获取信息的时间、速率、长度、来源及目的地。

4. 破坏数据的完整性

修改、插入、重放、删除用户数据或信令数据以破坏数据的完整性。

5. 拒绝服务

在物理上或协议上干扰用户数据、信令数据及控制数据在无线链路上的正确传输，实现拒绝服务攻击。

6. 否认

用户否认业务费用、业务数据来源及发送或接收到的其他用户的数据，网络单元否认提供的网络服务。

7. 非授权访问服务

用户滥用权限获取对非授权服务的访问，服务网滥用权限获取对非授权服务的访问。

8. 资源耗尽

通过使网络服务过载耗尽网络资源，使合法用户无法访问。

5.3.3　移动通信系统的安全机制

随着移动通信系统的不断发展，移动通信业务的不断增加，移动通信系统上传输的数据越来越重要，移动通信系统对安全方面的要求也越来越高。随着移动通信系统的发展，其安全机制也越来越强大，采用的安全技术水平也越来越高。

1. 第一代移动通信系统的安全机制

第一代移动通信系统的工作原理如图 5-17 所示。

第一代移动通信系统仅仅实现了一个简单的模拟语音的传输，其安全性能并不高，只是一个无机密性的保护机制。每个手机都有一个电子序号 ESN 和由网络编码的移动标识号

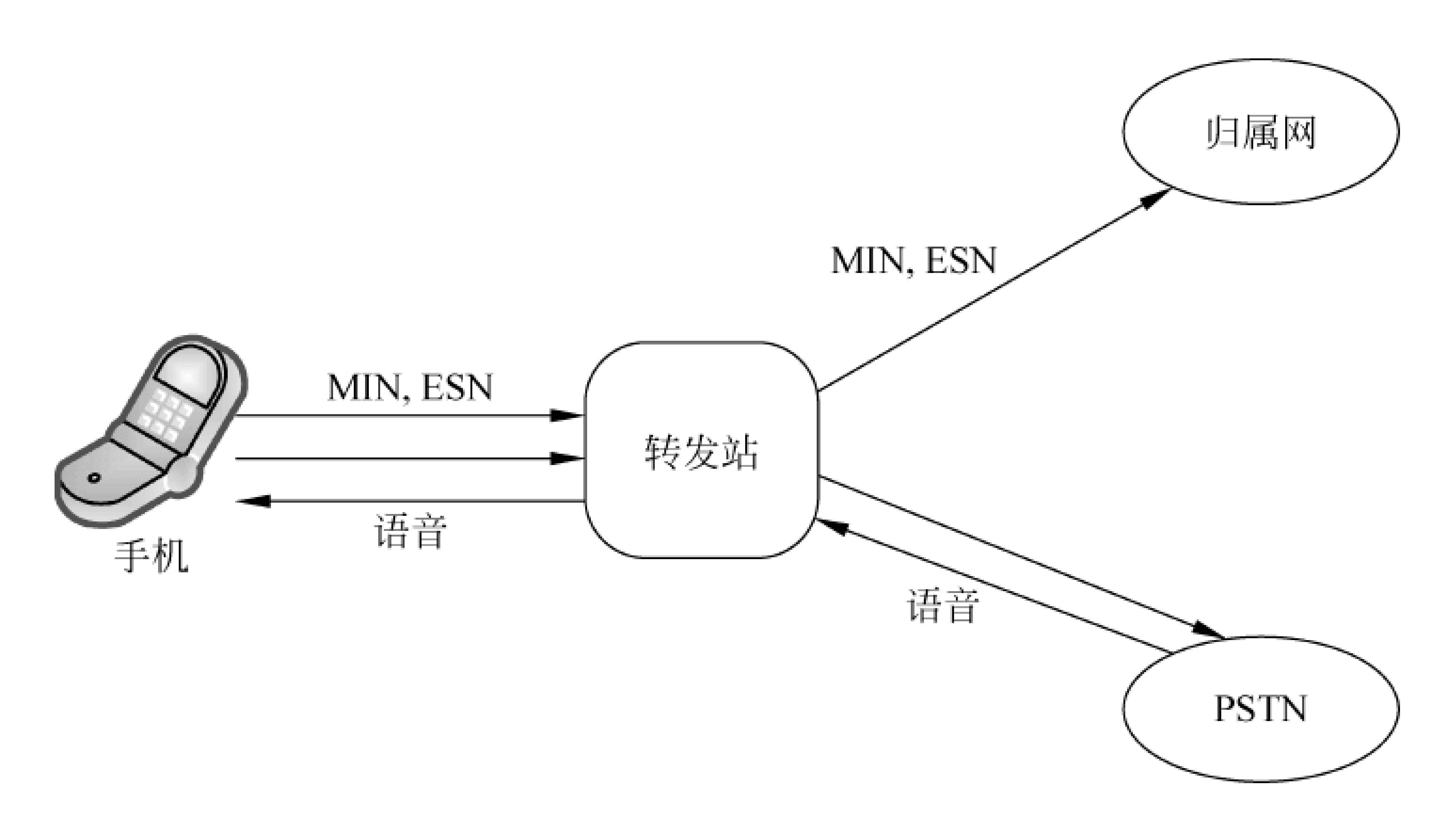


图 5-17　第一代移动通信系统的工作原理图

MIN。当用户接入的时候，手机只需要将 ESN 和 MIN 以明文的方式发送到网络，如果两者匹配，就能实现接入。通过上述的过程，可以看到只要监听无线电信号，就能够获取 ESN 和 MIN。利用窃取的 ESN 和 MIN，就可以不花任何费用拨打手机电话，这就是手机克隆。这种属于欺诈性的接入，给运营商带来了巨大的损失。频道劫持则是另外一种攻击手段，攻击者接管了正在进行通信的语音和数据会话。

2. 第二代移动通信系统的安全机制

第二代移动通信系统以 GSM 系统为代表，其网络结构如图 5-18 所示。

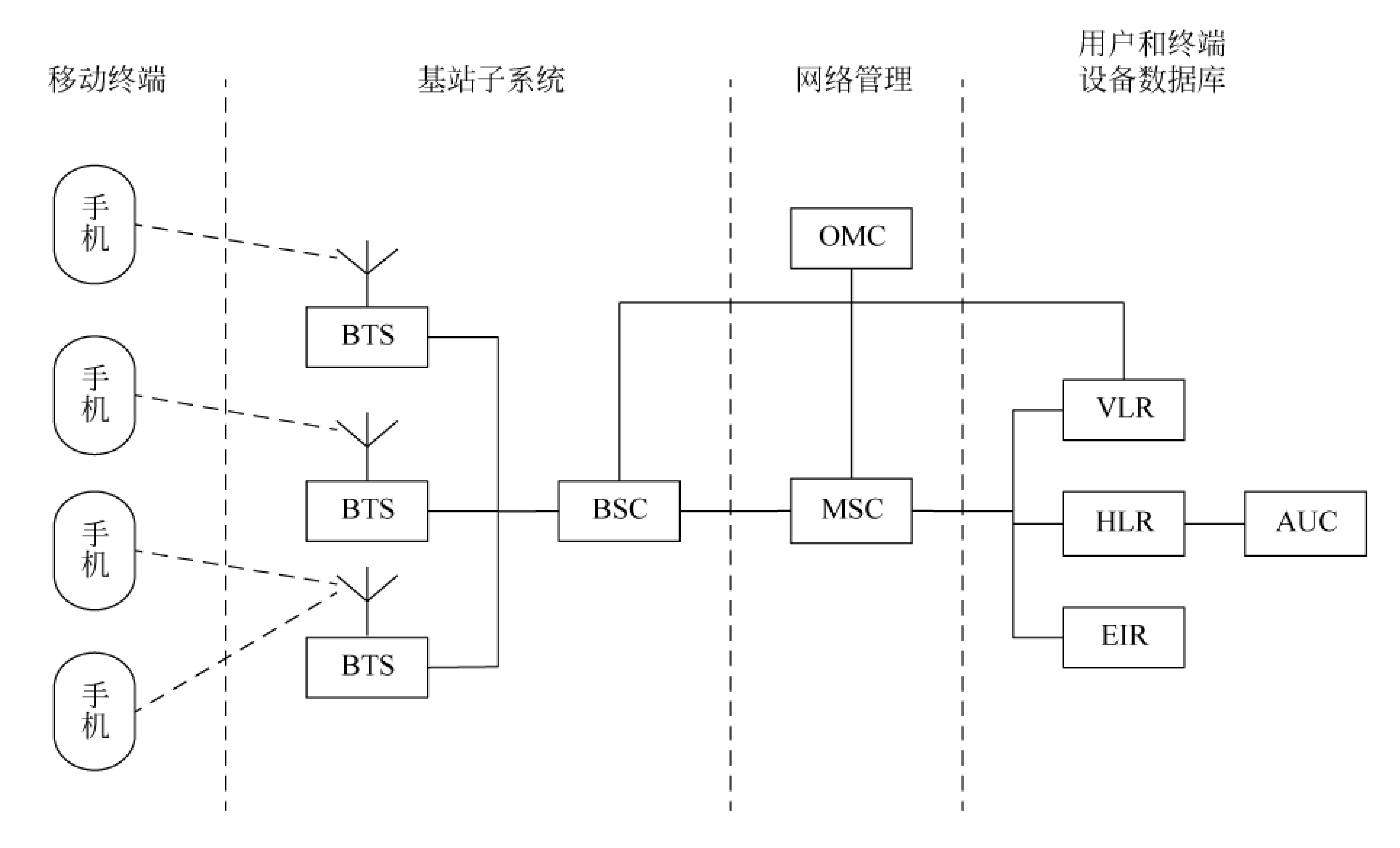


图 5-18　GSM 系统的网络结构

GSM 数字移动通信系统主要由移动交换系统、基站子系统（BSS）、操作维护子系统（OMS）和移动站（MS）构成。下面具体描述各部分的功能。

1）移动交换系统

移动交换系统主要完成交换功能以及用户数据管理、移动性管理、安全性管理所需的数据库功能。

移动交换系统由移动交换中心MSC、归属位置寄存器HLR、拜访位置寄存器VLR、设备识别寄存器EIR、鉴权中心AUC和短消息中心SMC等功能实体构成。

（1）MSC（Mobile Service Switching Center）即移动业务交换中，是GSM系统的核心，完成最基本的交换功能，即完成移动用户和其他网络用户之间的通信连接；完成移动用户寻呼接入、信道分配、呼叫接续、话务量控制、计费、基站管理等功能；提供面向系统其他功能实体的接口、到其他网络的接口以及与其他MSC互连的接口。

（2）HLR（Home Location Register）即归属位置寄存器，是GSM系统的中央数据库，存放与用户有关的所有信息，包括用户的漫游权限、基本业务、补充业务及当前位置信息等，从而为MSC提供建立呼叫所需的路由信息。一个HLR可以覆盖几个MSC服务区甚至整个移动网络。

（3）VLR（Visitor Location Register）即拜访者位置寄存器，VLR存储了进入其覆盖区的所有用户的信息，为已经登记的移动用户提供建立呼叫接续的条件。VLR是一个动态数据库，需要与有关的归属位置寄存器HLR进行大量的数据交换以保证数据的有效性。当用户离开该VLR的控制区域，则重新在另一个VLR登记，原VLR将删除临时记录的该移动用户数据。在物理上，MSC和VLR通常合为一体。

（4）AUC（AUthentication Center）即鉴权认证中心，是一个受到严格保护的数据库，存储用户的鉴权信息和加密参数。在物理实体上，AUC和HLR共存。

（5）EIR（Equipment Identity Register）即移动台设备识别寄存器，存储与移动台设备有关的参数，可以对移动设备进行识别、监视和闭锁等，防止未经许可的移动设备使用网络。

2）基站子系统BSS

基站子系统（Base Station System，BSS）是移动交换系统和MS之间的桥梁，主要完成无线信道管理和无线收发功能。BSS主要包括基站控制器BSC和基站收发信台BTS两部分。

（1）BSC（Base Station Controller）即基站控制器，位于MSC与BTS之间，具有对一个或多个BTS进行控制和管理的功能，主要完成无线信道的分配、BTS和MS发射功率的控制以及越区信道切换等功能。BSC也是一个小交换机，它把局部网络汇集后通过A接口与MSC相连。

（2）BTS（Base Transceiver Station）即基站收发信机，是基站子系统的无线收发设备，由BSC控制，主要负责无线传输功能，完成无线与有线的转换、无线分集、无线信道加密、跳频等功能。BTS通过Abis接口与BSC相连，通过空中接口Um与MS相连。

此外，BSS系统还包括码变换和速率适配单元TRAU。TRAU通常位于BSC和MSC之间，主要完成16 kbps的RPE-LTP编码和64 kbps的A律PCM编码之间的码型变换。

3）操作维护子系统OMS

OMS是GSM系统的操作维护部分，GSM系统的所有功能单元都可以通过各自的网络连接到OMS，通过OMS可以实现GSM网络各功能单元的监视、状态报告和故障诊断等功能。

OMS分为两部分：OMC-S(Operation and Maintenance Center-System)操作维护中心-系统部分和OMC-R(Operation and Maintenance Center-Radio)操作维护中心-无线部分。OMC-S用于NSS系统的操作和维护，OMC-R用于BSS系统的操作和维护。

4）移动站MS

MS(Mobile Station)移动站即手机，是GSM系统的用户设备，可以是车载台、便携台和手持机。它由移动终端和用户识别卡SIM两部分组成。移动终端主要完成语音信号处理和无线收发等功能。

SIM卡存储了认证用户身份所需的所有信息以及与安全保密有关的重要信息，以防非法用户入侵，移动终端只有插入了SIM卡后才能接入GSM网络。

第二代移动通信的安全缺陷主要包括：单项身份认证；使用明文进行传输，容易造成密钥的信息泄露；加密功能没有延伸到核心网；无法抗击重放攻击；没有消息完整性认证，无法保证数据在链路传输过程中的完整性；用户漫游时归属网络不知道和无法控制服务网络，如何使用自己用户的认证参数；没有第三方仲裁功能；系统安全缺乏升级能力等。

3. 第三代移动通信系统的安全机制

第三代移动通信系统在2G的基础上进行了改进，继承了2G系统安全的优点，同时针对3G系统的新特性，定义了更加完善的安全特征与安全服务。未来的移动通信系统除了提供传统的语音、数据、多媒体业务外，还应当能支持电子商务、电子支付、股票交易、互联网业务等，个人智能终端将获得广泛使用，网络和传输信息的安全将成为制约其发展的首要问题。

随着向下一代网络(NGN)的演进，基于IP的网络架构必将使移动网络面临IP网络固有的一些安全问题。移动通信网络最终会演变成开放式的网络，能向用户提供开放式的应用程序接口，以满足用户的个性化需求。网络的开放性以及无线传播的特性将使安全问题成为整个移动通信系统的核心问题之一。

与2G以语音业务为主、仅提供少量的数据业务不同，3G可提供高达2Mbit/s的无线数据接入方式。其安全模式也以数据、交互式、分布式业务为主。

1）第三代移动通信系统的网络结构

第三代移动通信系统的网络结构如图5-19所示。

第三代移动通信系统由三部分组成：移动终端、无线接入网(Radio Access Network，RAN)和核心网(Core Network，CN)。

(1）移动终端。

移动终端由两个部分组成：移动设备(Mobile Equipment，ME)和全球用户识别模块(Universal Subscriber Identity Module，USIM)。移动设备实现无线通信功能，全球用户识别模块与SIM卡类似，保存了与运营商相关的用户信息。

(2）无线接入网。

3G中包括两种无线接入网，即地面无线接入网络(UMTS Terrestrial Radio Access Network，UTRAN)和GSM/EDGE无线接入网络(GSM/EDGE Radio Access Network，GERAN)。地面无线接入网络含有两种网络单元：BS是RAN在网络一侧的终点，BS被连接到UTRAN的控制单元(如无线网络控制单元RNC)上。RNC则通过Iu接口与CN

相连。

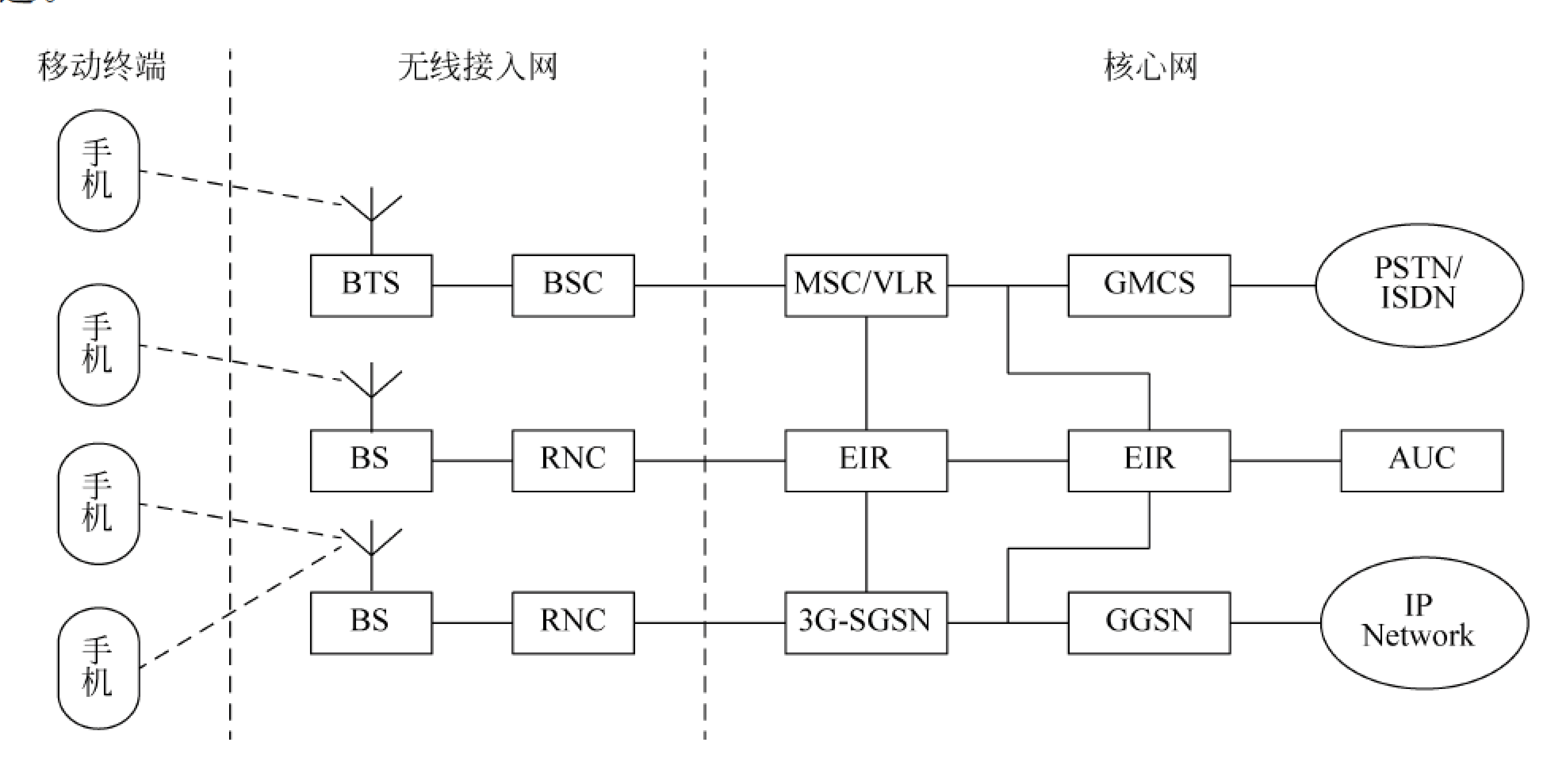


图 5-19 第三代移动通信系统的网络结构

(3) 核心网。

核心网(Core Network,CN)主要有两个域：分组交换(Packet Switch)域和电路交换(Circuit Switch)域。分组交换域是从GPRS域进化而来的,其中重要的网络单元是GPRS服务支持结点SGSN和GPRS网关支持结点GGSN。CS也是从传统的GSM网络进化而来,其中重要的网络单元是MSC。SGSN和GGSN是GPRS中新增加的网络单元,SGSN的主要作用是记录移动终端的当前位置信息,并且在移动终端与GGSN之间完成移动分组数据的发送和接收。GGSN通过基于IP的GPRS骨干网连接到SGSN,然后连接到GSM网络和外部交换网。核心网还可以分为两部分：本地网络和服务网,本地网络包含所有用户的静态信息,服务网则处理用户设备到接入网之间的通信。

2) 3G系统的安全体系

3GPP的接入安全规范已经成熟,加密算法和完整性算法已经实现标准化。基于IP的网络域的安全也已制定出相应的规范。3GPP的终端安全、网络安全管理规范还有待进一步完善。

为实现3G安全特征的目标,应针对它面临的各种安全威胁和攻击,从整体上研究和实施3G系统的安全措施,只有这样才能有效保障3G系统的信息安全。

如图5-20所示,给出了一个完整的3G系统的安全体系。

在3G系统的安全体系中,针对不同的攻击类型,分别定义了五个安全特征组,即网络接入安全(Ⅰ)、核心网安全(Ⅱ)、用户域安全(Ⅲ)、应用域安全(Ⅳ)、安全的可知性及可配置性(Ⅴ)。它们涉及传输层、归属层/服务层和应用层,同时也涉及移动用户(包括移动设备MS)、服务网和归属环境。每一安全特征组用以对抗某些威胁和攻击,实现3G系统的某些安全目标。

(1) 网络接入安全。

该安全特征组提供用户安全接入3G业务,特别是对抗在无线接入链路上的攻击。

(2) 核心网安全。

该安全特征组使网络运营商之间的结点能够安全交换信令数据,对抗在有限网络上的

攻击。

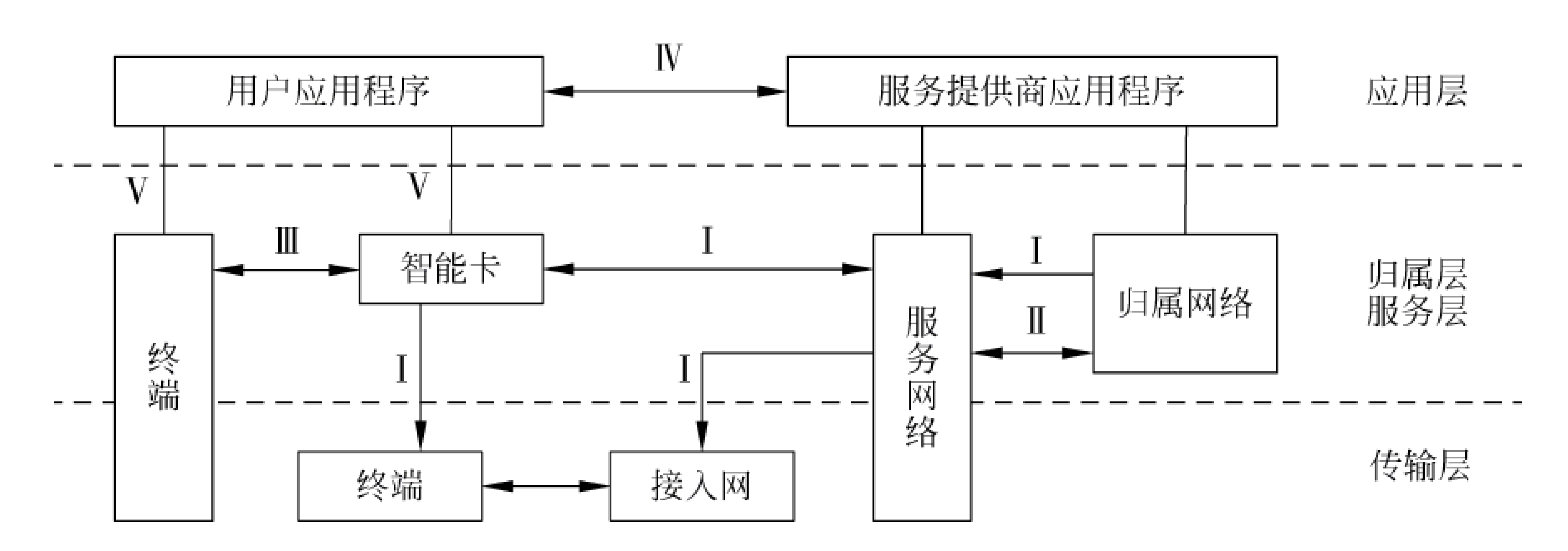


图 5-20　3G 系统的安全体系

(3) 用户域安全。

该安全特征组确保用户能够安全接入网络。

(4) 应用域安全。

该安全特征组使得用户和网络运营商之间的各项应用能够安全交换信息。

(5) 安全的可知性及可配置性。

该安全特征组使得用户能够知道某个安全特征组是否在运行,并且业务的应用和设置是否依赖于该安全特征。

3) 3G 系统的接入安全机制

3G 系统的接入安全机制有三种:根据临时身份(TMSI)识别;根据永久身份(IMSI)识别;认证和密钥协商(AKA)。

AKA 机制完成移动终端(MS)和网络的相互认证,并建立新的加密密钥和完整性密钥。AKA 机制的执行分为两个阶段:第一阶段是认证向量(AV)从归属环境(HE)到服务网络(SN)的传送;第二阶段是 SGSN/VLR 和 MS 执行询问应答程序取得相互认证。HE 包括 HLR 和鉴权中心(AUC)。认证向量含有与认证和密钥分配有关的敏感信息,在网络域的传送使用基于七号信令的 MAPsec 协议,该协议提供了数据来源认证、数据完整性、抗重放和机密性保护等功能。

4) 3G 安全算法

3G 系统定义了多种安全算法:f0、f1、f2、f3、f4、f5、f6、f7、f8、f9、f1*、f5*,应用于不同的安全服务。身份认证与密钥分配方案中移动用户登记和认证参数的调用过程与 GSM 网络基本相同,不同之处在于 3GPP 认证向量是 5 元组,并实现了用户对网络的认证。AKA 利用 f0 至 f5* 算法,这些算法仅在鉴权中心和用户的用户身份识别模块(USIM)中执行。

其中,f0 算法仅在鉴权中心中执行,用于产生随机数 RAND;f1 算法用于产生消息认证码(鉴权中心中为 MAC-A,用户身份识别模块中为 XMAC-A);f1* 是重同步消息认证算法,用于产生 MAC-S;f2 算法用于产生期望的认证应答(鉴权中心中为 XRES,用户身份识别模块中为 RES);f3 算法用于产生加密密钥 CK;f4 算法用于产生消息完整性密钥 IK;f5 算法用于产生匿名密钥 AK 和对序列号 SQN 加解密,以防止被位置跟踪;f5* 是重同步时的匿名密钥生成算法。

AKA 由 SGSN/VLR 发起,在鉴权中心中产生认证向量 AV=(RAND,XRES,CK,

IK,AUTN)和认证令牌 AUTN=SQN[AAK]‖AMF‖MAC-A。VLR 发送 RAND 和 AUTN 至用户身份识别模块。用户身份识别模块计算 XMAC-A=f1K(SQN‖RAND‖AMF),若等于 AUTN 中的 MAC-A,并且 SQN 在有效范围,则认为对网络鉴权成功,计算 RES、CK、IK,发送 RES 至 VLR。VLR 验证 RES,若与 XRES 相符,则认为对 MS 鉴权成功;否则,拒绝 MS 接入。当 SQN 不在有效范围时,用户身份识别模块和鉴权中心利用 f1*算法进入重新同步程序,SGSN/VLR 向 HLR/AUC 请求新的认证向量。

3G 的数据加密机制将加密保护延长至无线接入控制器(RNC)。数据加密使用 f8 算法,生成密钥流块 KEYSTREAM。对于 MS 和网络间发送的控制信令信息,使用算法 f9 来验证信令消息的完整性。对于用户数据和话音不给予完整性保护。MS 和网络相互认证成功后,用户身份识别模块和 VLR 分别将 CK 和 IK 传给移动设备和无线网络控制器,在移动设备和无线网络控制器之间建立起保密链路。f8 和 f9 算法都是以分组密码算法 KASUMI 构造的,KASUMI 算法的输入和输出都是 64bit,密钥是 128bit。KASUMI 算法在设计上具有对抗差分和线性密码分析的可证明的安全性。

5）第三代移动通信系统安全机制的优点

相对于 2G 移动通信系统,3G 系统具有以下优点:

(1) 提供了双向认证。不但提供基站对 MS 的认证,也提供了 MS 对基站的认证,可有效防止伪基站攻击。

(2) 提供了接入链路信令数据的完整性保护。

(3) 密码长度增加为 128bit,改进了算法。

(4) 3GPP 接入链路数据加密延伸至 RNC。

(5) 3G 的安全机制还具有可拓展性,为将来引入新业务提供安全保护措施。

(6) 3G 能向用户提供安全可视性操作,用户可随时查看自己所用的安全模式及安全级别。

6）第三代移动通信系统安全机制的缺点

在密钥长度、算法选定、鉴别机制和数据完整性检验等方面,3G 的安全性能远远优于 2G。但 3G 仍然存在下列安全缺陷:

(1) 没有建立公钥密码体制,难以实现用户数字签名。随着移动终端存储器容量的增大和 CPU 处理能力的提高以及无线传输带宽的增加,必须着手建设无线公钥基础设施(WPKI)。

(2) 密码学的最新成果(比如 ECC 椭圆曲线密码算法)并未在 3G 中得到应用。

(3) 算法过多。

(4) 密钥产生机制和认证协议有一定的安全隐患。

4. 第四代移动通信系统的安全机制

1）网络结构

第四代移动通信系统的网络结构如图 5-21 所示。4G 系统包括移动终端、无线接入网、无线核心网和 IP 骨干网等四个部分。

4G 网络实现了不同固定和无线平台以及跨越不同频带的无线网络的连接,为所连接的无线平台和无线网络提供了无缝的、一致性的移动计算环境,并支持高速移动环境下数据的

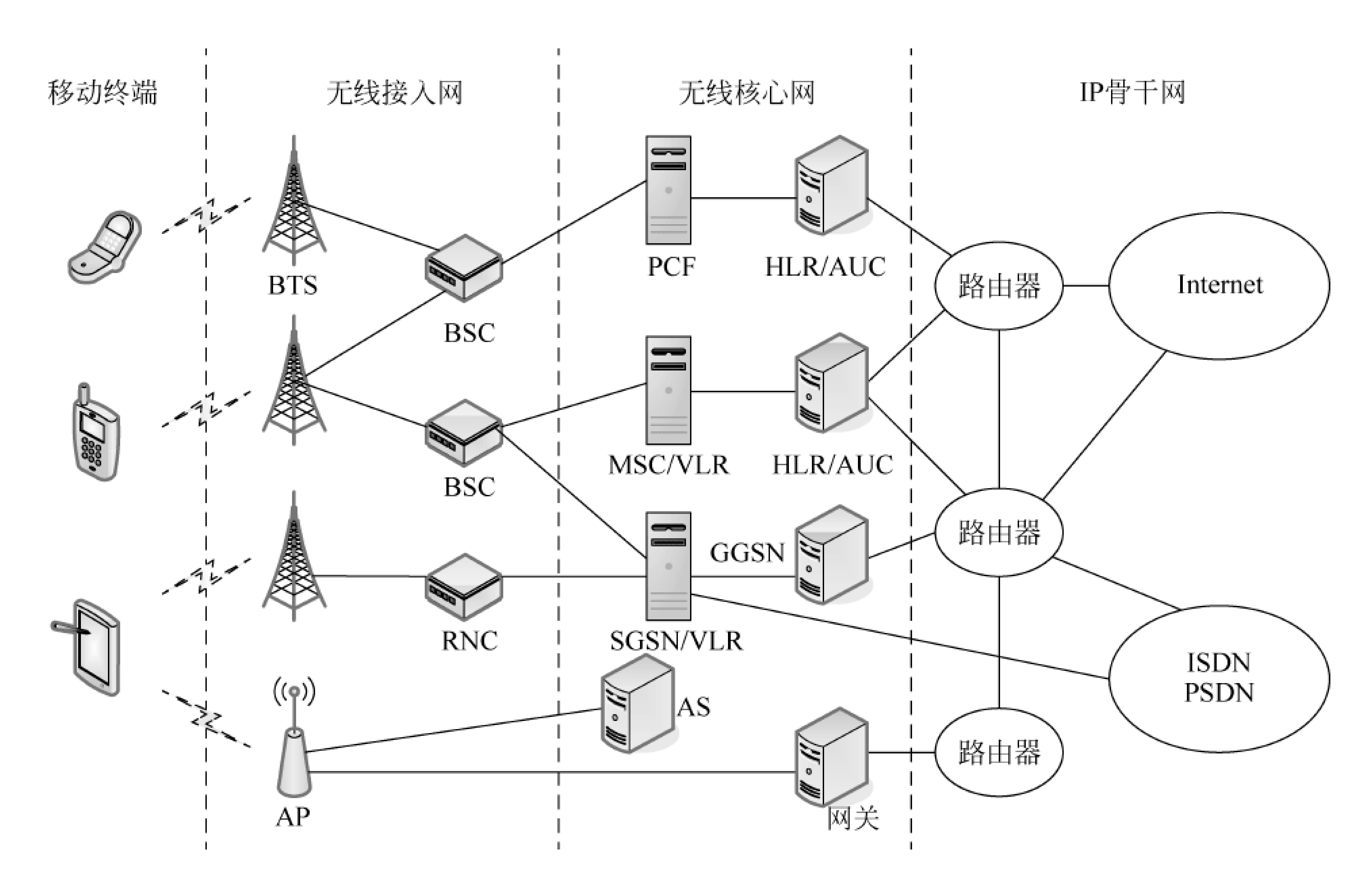


图 5-21　第四代移动通信系统的网络结构

高速传输功能,能够对语音、数据、图像进行高质量、高速度的传输。4G 网络将固定的有线网络与无线蜂窝网络、卫星网络、广播电视网络、蓝牙等系统集成和融合,这些接入网络都将被无缝地接入基于 IP 的核心网,形成一个公共的平台,这个平台较之于传统的平台将具有更高的公共性、灵活性、可扩展性。

2) 第四代移动通信系统的特点

第四代移动通信系统的主要特点如下:

(1) 多网络集成:4G 网络集成和融合多种网络和无线通信技术系统。

(2) 全 IP 网络:4G 网络是一种基于分组的全 IP 网络。

(3) 大容量:4G 网络的容量较之于 3G 网络要大得多,大约是其 10 倍左右。

(4) 无缝覆盖:4G 网络实现了无缝覆盖,用户可以在任何时间、任何地点使用无线网络。

(5) 带宽更宽:每个 4G 信道将占有较之于 3G 信道约 20 倍宽度的频谱。

(6) 高灵活性和扩展性:4G 网络可以通过与其他网络的自由连接来扩展自身的范围,同时网络中的用户和网络设备可以自由增减。

(7) 高智能性:4G 网络实现了终端设备设计和操作的智能化,可以自适应地进行资源分配、业务处理和信道环境适应。

(8) 高兼容性:4G 网络采用的是开放性的接口,可以实现多网络互联、多用户融合。

3) 第四代移动通信系统面临的安全问题

随着通信技术的迅速发展,我国也已经进入到 4G 的潮流之中,但是随着在 4G 通信技术的日益发展,其漏洞也日益暴露,引发了一系列的安全问题。其中,最主要的安全问题包括在 4G 网络规模的扩大、通信技术以及相关业务的不断发展和来自外部网络的安全威胁。

网络规模的扩大,顾名思义,是指网络的使用范围的扩展面积较大,网络的管理系统已

经跟不上网络拓展的步伐，这样就导致在管理方面存在着较大的问题。

来自外部网络的安全威胁也不忽视，这些威胁主要包括网络病毒的传播以及 4G 网络存在的相关漏洞导致黑客入侵等方面。其中，仅仅是手机病毒，就存在着很多的安全威胁。手机病毒可以分为短信息类手机病毒、蠕虫类手机病毒以及常见的木马类手机病毒，这些来自于外界的网络安全危害，都会对在 4G 网络造成威胁等，这些问题的存在将严重制约 4G 网络技术安全的拓展，同时也不利于我国通信技术的发展。

目前，我国的 4G 网络技术尚处于起步阶段，尚未建立有效的统一化管理，同时 4G 网络安全技术还难以与其他的移动通信相兼容，难于做到与全球移动通信设备进行安全的、无缝隙的漫游，这样会使得移动用户在使用上产生诸多的不便。

4G 网络技术是 3G 网络的升级版本，但是 4G 网络技术并未达到相关的技术要求，在 3G 网络技术的覆盖区域尚未达到全面的覆盖，两个覆盖的区域不能相互兼容，同时难以保证 4G 网络技术的覆盖区域的安全性能。

通信系统容量的限制，也大大制约着手机的下载速度，虽然 4G 网络技术的下载速度要比 3G 的速度快很多，但是受 4G 网络技术系统限制的同时手机用户不断地增加，网络的下载速度将会逐渐降低，同时下载的文件是否都具备安全的性能也不能保证，因此如何解决这一问题，将是被列为保证 4G 网络安全发展研究的重要解决问题之一。

4）4G 网络的安全对策

目前，4G 网络最大的安全问题是在应用领域上存在的安全隐患，一旦这些问题出现将带来非常严重的后果。因此，需要与 4G 网络相关的所有成员共同关注。第一，开发商要加强 4G 网络安全机制的研发工作；第二，运营商应当采取严格的安全防护措施；第三，4G 网络用户也要提高自身的安全防范意识。针对 4G 网络的安全对策如下：

（1）建立安全的移动通信系统。

要推进 4G 网络技术不断发展，就要做好相关的安全措施，分析 4G 网络的安全需求，确定 4G 网络安全的目标，保证移动平台硬件与应用软件以及操作系统的完整性，明确使用者的身份权限，并保证用户的隐私安全。

（2）建立安全认证体系。

目前的移动通信安全体制，通常都采用私钥密码的单一体制。但是这样的私钥密码体制难以全方位地保证 4G 网络的安全。应当针对不同的安全特征与服务，采用公钥密码体制和私钥密码体制的混合，与此同时加快公钥的无线基础设施建设，建立以 CA 为认证中的核心安全认证体系。

（3）发展新型的 4G 网络加密技术。

要推进 4G 网络技术安全的发展，就必须发展新型的 4G 网络加密技术，如量子密码技术、椭圆曲线密码技术、生物识别技术等移动通信系统加密技术，提高加密算法和认证算法的自身抗攻击能力，保证 4G 网络技术在传输机密信息时的完整性、可控制性、不可否认性以及可用性。

（4）加强 4G 网络安全的防范意识。

单纯地依靠开发商、网络管理者的努力是不够的。用户能否安全地使用 4G 网络，更是在 4G 网络技术发展中最不容忽视的重要环节。

为了促进 4G 网络的发展，用户自身应该加强自身的安全防范意识。例如，不访问不安

全的钓鱼网站；不到盗版网站下载有可能存在病毒的文件；定期地清理手机中的垃圾；定期查杀病毒等。

5.4 本章小结

国际互联网或下一代网络(IPv6)是物联网网络层的核心载体。在物联网中，原来在国际互联网遇到的各种攻击问题依然存在，甚至更普遍，因此物联网需要有更完善的安全防护机制。

目前的物联网核心网主要是运营商的核心网络，核心网安全防护系统可以为物联网终端设备提供本地和网络应用的身份认证、网络过滤、访问控制、授权管理等安全服务。核心网的安全防护技术主要涉及网络加密技术、防火墙技术、隧道技术、网络虚拟化技术、黑客攻击与防范、计算机病毒防护、入侵检测技术、网络安全扫描技术等。

防火墙技术是一种隔离控制技术，在某个机构的网络和不安全的网络(如 Internet)之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止重要信息从企业的网络上被非法输出。

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

网络虚拟化一般指虚拟专用网络(Virtual Private Network，VPN)。VPN 对网络连接的概念进行了抽象，允许远程用户访问组织的内部网络，就像物理上连接到该网络一样。网络虚拟化可以帮助保护 IT 环境，防止来自 Internet 的威胁，同时使用户能够快速安全的访问应用程序和数据。

黑客一般是指网络的非法入侵者，他们往往是优秀的程序员，具有计算机网络和物联网的软件及硬件的高级知识，并有能力通过一些特殊的方法剖析和攻击网络。黑客以破坏网络系统为目的，往往采用某些不正当的手段找出网络的漏洞，并利用网络漏洞破坏计算机网络或物联网，从而危害网络的安全。

针对黑客各种不同的攻击行为，网络管理员可以采取的防御对策包括：屏蔽可疑的 IP 地址、过滤信息包、修改系统协议、修补安全漏洞、及时备份重要数据、使用加密机制传输数据和安装安全软件等。

计算机病毒是编制者在计算机程序中插入的破坏计算机网络功能或者数据的代码，能影响计算机网络的使用，能自我复制的一组计算机指令或者程序代码。

计算机病毒具有传染性、繁殖性、潜伏性、隐蔽性、可触发性和破坏性等特征。

为了保证物联网的正常运行，阻止计算机病毒或者流氓软件入侵物联网系统，物联网用户应当采取的防御措施包括：不要随便浏览陌生的网站、安装杀毒软件、安装防火墙、及时安装系统漏洞补丁、不要轻易打开陌生的电子邮件附件、使用 U 盘时要先杀毒、对下载的文件进行杀病毒和及时备份等。

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。

进行入侵检测的软件与硬件相结合，便构成了入侵检测系统（Intrusion Detection System，IDS）。

扫描工具是一种利用网络安全扫描技术自动地检测目标主机安全弱点的程序。它能够发现目标主机开放的端口和运行的服务，是否存在系统漏洞和安全弱点等。它通过与目标主机开放的端口建立连接或请求服务，如http、telnet等，获取目标主机的应答信息，以搜集相关的信息，如操作系统类型等，从而发现目标主机存在的安全弱点。它是一把双刃剑，利用网络安全扫描工具的扫描结果，可以为攻击目标网络系统提供指导，同时还可以用于网络系统的安全评测，评估网络系统的安全性，对系统存在的漏洞提出修补建议。因此，网络安全扫描工具既是网络攻击的重要武器之一，同时也是网络安全防御的重要手段之一。

无线局域网一般用于较小范围的无线通信，覆盖范围比较小，一般为一栋建筑物内或房间内，采用IEEE 802.11系列标准，传输速率，一般在11～56Mbps之间，连接距离一般限制在50～100m，工作频段为2.4GHz。

无线局域网产品面临的安全隐患主要有容易入侵、非法的接入点、未经授权使用服务、服务和性能的限制、地址欺骗和会话拦截、流量分析与流量侦听、高级入侵等几种。

到目前为止，已经有很多种无线局域网的安全技术，包括物理地址过滤、服务区标识符（SSID）匹配、有线对等保密（WEP）、端口访问控制技术、WPA、IEEE 802.11i和WAPI等。

IEEE的802.16标准是用来标准化空中接口和无线本地环路与耦合的相关功能，它是一种无线城域网的革命性标准，可以为数据、视频和语音业务提供高速的无线接入服务。IEEE 802.16的主要目的是提供宽带无线接入，因此它被认为是一种取代xDSL等有限宽带接入的有力替代者。该标准的主要优势在于可以快速、灵活地进行网络部署，从而降低了网络的建设成本。对于城市等人口密集区域和农村等没有有线网络基础的网络建设，无线宽带接入设备的优势是非常明显的。

WiMAX/802.16网络体系包括：核心网、用户基站（SS）、基站（BS）、中继站（RS）、用户终端设备（TE）和网管。

蓝牙技术是一个开放性、短距离无线通信的标准，它可以用在较短距离内取代多种有线电缆连接方案，通过统一的短距离无线链路在各种数字设备之间实现方便、快捷、灵活、安全、低成本、小功耗的语音和数据通信。

蓝牙标准体系中的协议按特别兴趣小组SIG的关注程度分为四层：核心协议、串口仿真协议（RFCOMM）、电话控制协议（Telephone Control Protocol Specification，TCS）和选用协议。

蓝牙标准中定义了3种网络安全模式：非安全模式、强制业务级安全模式和强制链路级安全模式。

蓝牙安全体系中主要使用3种密钥以确保安全的数据传输：个人识别码（PIN）、链路密钥和加密密钥。其中最重要的是链路密钥，用于两个蓝牙设备之间的相互鉴别。

ZigBee技术是可以实现短距离无线通信的新兴技术，它以功耗低、成本低、复杂程度低优胜于其他的短距离无线通信技术。

ZigBee技术的主要特点包括：功耗低、成本低、较小的传输范围、时延短、网络容量大、数据传输时的可靠性较高、安全性高等。

ZigBee建立在IEEE 802.15.4标准之上，它确定了可在不同制造商之间共享的应用纲

要。IEEE 802.15.4 仅定义了物理层和数据链路层。

ZigBee 兼容的产品工作在 IEEE 802.15.4 的物理层之上，可以工作在全球通用标准的 2.4GHz、美国标准的 915MHz 和欧洲标准的 868MHz 三个的频段上，并且在这三个频段上分别具有 250kbps、40kbps 和 20kbps 的最高数据传输速率。

IEEE 802.15.4 的 MAC 协议包括以下功能：设备之间无线链路的建立、维护和结束；确认模式的帧传输与接收；信道接入控制；帧校验；预留时隙管理；广播信息管理等。同时，使用 CSMA-CA 机制和应答重传机制，实现了信道的共享及数据帧的可靠传输。

ZigBee 网络层的主要功能是负责拓扑结构的建立和网络连接的维护，包括设计连接和断开网络时所采用的机制、帧传输过程中所采用的安全性机制、设备的路由发现和转交机制等。

ZigBee 应用层主要负责把不同的应用映射到 ZigBee 网络，主要包括三部分：与网络层连接的应用支持子层（Application Support Sublayer，APS）、ZigBee 设备对象（ZigBee Device Object，ZDO）和 ZigBee 的应用层框架（Application Framework，AF）。

超宽带（UWB）技术起源于 20 世纪 50 年代末，早期主要作为军事技术在雷达探测和定位等应用领域中使用。UWB 通信技术的主要特点有低成本、传输速率高、空间容量大和低功耗等。

超宽带面临的信息安全威胁包括：拒绝服务攻击、密钥泄露、假冒攻击和路由攻击。

针对超宽带网络应用过程中容易发生的信息安全问题，国际标准化组织接受了由 WiMedia 联盟提出的《高速率超宽带通信的物理层和媒体接入控制标准》，即 ECMA-368（ISO/IEC26907），它规范了相应的安全性要求。

ECMA-368（ISO/IEC26907）标准定义了两种安全级别：无安全和强安全保护。安全保护包括数据加密、消息认证和重播攻击防护；安全帧提供对数据帧、选择帧和控制帧的保护。

ECMA-368（ISO/IEC26907）标准定义了三种安全模式，用于控制设备间的通信。两台设备通过四次握手协议来建立安全关系。一旦两台设备建立了安全关系，它们将使用安全帧来作为数据帧，如果接收方需要接收安全帧，而发送方无安全帧，那么接收方将丢弃该帧。

到目前为止，移动通信系统的发展已经经历了四个时代。

第一代移动通信系统简称为 1G，主要采用蜂窝组网和频分多址（FDMA）技术。由于受到传输带宽的限制，不能进行移动通信的长途漫游，只能是一种区域性的移动通信系统。第一代移动通信有多种制式，我国主要采用的是 TACS。

第二代移动通信系统以传输话音和低速数据业务为目的，因此又称为窄带数字通信系统。第二代数字蜂窝移动通信系统的典型代表是美国的 DAMPS 系统、IS-95 系统和欧洲的 GSM 系统。

第三代移动通信系统能够同时传送声音及数据信息，速率一般在几百 kbps 以上。3G 是指将无线通信与国际互联网等多媒体通信结合的新一代移动通信系统，目前 3G 存在 3 种标准：CDMA2000、WCDMA、TD-SCDMA。

第四代移动通信系统集 LTE 技术与 WiMAX 技术于一体，并能够快速传输数据、高质量、音频、视频和图像等。4G 能够以 100Mbps 的峰值速率下载，比目前的家用宽带 ADSL 快 25 倍，并能够满足几乎所有用户对于无线服务的要求。此外，4G 可以在 DSL 和有线电

视调制解调器没有覆盖的地方部署,然后再扩展到整个地区。

移动通信系统面临的安全威胁来自网络协议和系统的弱点,攻击者可以利用网络协议和系统的弱点非授权访问敏感数据、非授权处理敏感数据、干扰或滥用网络服务,对用户和网络资源造成损失。

第一代移动通信系统仅仅实现了一个简单的模拟语音的传输,其安全性能并不高,只是一个无机密性的保护机制。

在 GSM 系统中,为了实现安全特性和目标,主要采取了以下安全措施:在接入网络方面采用对用户鉴权;在无线链路上采用对通信信息加密;用户身份鉴别采用临时识别码(TMSI)保护;对移动设备采用设备识别;SIM 卡用 PIN 码保护。

WCDMA、TD-SCDMA 的安全规范由以欧洲为主体的 3GPP 制定,CDMA2000 的安全规范由以北美为首的 3GPP2 制定。

与 2G 以语音业务为主、仅提供少量的数据业务不同,3G 可提供高达 2Mbps 的无线数据接入方式。其安全模式也以数据、交互式、分布式业务为主。

保证 4G 网络技术安全发展给予实施的措施包括:建立移动通信系统的安全机制、密码体制的改进以及完善安全认证体系、发展新型的 4G 网络加密技术、加强 4G 网络技术安全的防范意识等。

复习思考题

1. 物联网网络层安全主要涉及哪些安全技术?
2. 什么是防火墙?
3. 从工作原理来分类,防火墙技术可以分为哪些类别?
4. 防火墙具有哪些功能?
5. 什么网络虚拟化技术?
6. 什么是隧道技术? 常见的隧道技术包括哪些?
7. 请简要说明 IPSec 隧道技术的工作原理。
8. 什么是黑客? 黑客常用的攻击方法包括哪些?
9. 防范黑客攻击主要有哪些对策?
10. 什么是计算机病毒? 计算机病毒具有哪些特征?
11. 计算机病毒如何分类?
12. 为了阻止计算机病毒的感染,应采取哪些预防措施?
13. 什么是入侵检测技术? 入侵检测的过程分为哪些步骤?
14. 请画图表示 CIDF 提出的入侵检测系统的通用模型。
15. 常用的入侵检测系统检测方法包括哪些?
16. 网络安全扫描技术主要包括哪些技术?
17. 无线局域网的特点和主要标准是什么? 无线局域网具有什么优点?
18. 无线局域网的安全隐患包括哪些方面?
19. 无线局域网包括哪些安全技术?
20. 蓝牙技术的特点是什么?

21. 蓝牙标准体系中的协议包括哪些协议?

22. 请画图说明微微网(Piconet)和散射网络(Scatternet)。

23. 蓝牙标准中定义了哪几种网络安全模式?

24. 蓝牙安全体系中主要使用哪些密钥以确保安全的数据传输? 其中最重要的是哪种密钥?

25. ZigBee 技术的主要特点是什么?

26. 请分别从物理层、数据链路层、网络层、应用层分析 ZigBee 技术标准。

27. 超宽带通信技术的主要特点是什么?

28. 超宽带面临哪些信息安全威胁?

29. ECMA-368(ISO/IEC26907)标准的主要内容是什么?

30. 针对 UWB 网络中基于数据报文的拒绝服务攻击,可以采用什么防御措施?

31. 移动通信系统的发展已经经历了哪些时代?

32. 中国的 3 个 3G 无线接口标准是什么? 各有什么特点?

33. 第四代移动通信系统的特点是什么?

34. 移动通信系统面临的安全威胁是什么?

35. 第一代移动通信系统的安全机制是什么?

36. 请画图说明 GSM 系统的网络结构。

37. 第二代移动通信系统的安全机制是什么?

38. 第三代移动通信系统的安全机制是什么?

39. 第四代移动通信系统的特点是什么?

40. 4G 网络技术面临的安全问题是什么?

41. 保证 4G 网络安全包括哪些措施?

第6章 应用层安全技术

6.1 云计算安全

6.1.1 云计算概述

1. 云计算思想的产生

传统模式下,企业建立一套 IT 系统不仅仅需要购买硬件等基础设施,还有购买软件的许可证,需要专门的人员维护。当企业的规模扩大时还要继续升级各种软硬件设施以满足需要。对于企业来说,计算机等硬件和软件本身并非他们真正需要的,它们仅仅是完成工作、提供效率的工具而已。对个人来说,电脑需要安装许多软件,而许多软件是收费的,对不经常使用该软件的用户来说购买是非常不划算的。那么,能否由厂商提供这样的服务,使我们可以租用而不是购买所需要的软件?这样我们只需要在使用时付少量“租金”即可,从而节省许多购买软硬件的资金。

我们每天都要用电,但我们不是每家自备发电机,它由电厂集中提供;我们每天都要用自来水,但我们不是每家都有井,它由自来水厂集中提供。这种模式极大地节约了资源,方便了我们的生活。面对计算机给我们带来的困扰,我们可不可以像使用水和电一样使用计算机资源?这些想法最终导致了云计算的产生。

云计算的最终目标是将计算、服务和应用作为一种公共设施提供给公众,使人们能够像使用水、电、煤气和电话那样使用计算机资源。

云计算模式与电厂集中供电模式类似。在云计算模式下,用户的计算机会变得十分简单,或许不大的内存、不需要硬盘和各种应用软件,就可以满足我们的需求,因为用户的计算机除了通过浏览器给“云”发送指令和接收数据外基本上什么都不用做便可以使用云服务提供商的计算资源、存储空间和各种应用软件。这就像连接“显示器”和“主机”的电线无限长,从而可以把显示器放在使用者的面前,而主机放在远到甚至计算机使用者本人也不知道的地方。云计算把连接“显示器”和“主机”的电线变成了网络,把“主机”变成云服务提供商的服务器集群。

在云计算环境下,用户的使用观念也会发生彻底的变化:从“购买产品”到“购买服务”转变,因为他们直接面对的将不再是复杂的硬件和软件,而是最终的服务。用户不需要拥有看得见、摸得着的硬件设施,也不需要为机房支付设备供电、空调制冷、专人维护等等费用,

并且不需要等待漫长的供货周期、项目实施等冗长的时间，只需要把钱汇给云计算服务提供商，我们将会马上得到需要的服务。

2．云计算的概念

云计算是一种新兴的商业计算模型，它利用高速互联网的传输能力，将数据的处理过程从个人计算机或服务器转移到一个大型的计算中心，并将计算能力、存储能力当作服务来提供，就如同电力、自来水一样按使用量进行计费。

云计算基本原理是计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，从而使企业数据中心的运行与互联网相似。这使企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

云计算的核心是新一代数据中心技术，包括绿色IT、高性能（网格）计算、分布式计算以及数据中心虚拟化等。云计算作为传统计算机技术与网络融合的产物，可以将各类资源以服务的形式向用户提供，具有可虚拟化性、动态性和可伸缩性，被认为是信息产业的又一次重大革命。虚拟化及虚拟机概念是20世纪60年代由IBM提出，主要通过将有限的固定的资源根据不同需求进行重新规划以达到简化管理，优化资源的目的。

“云”是一些可以自我维护和管理的虚拟计算资源，通常为一些大型服务器集群，包括计算服务器、存储服务器、Web服务器、宽带资源等等。云计算将所有的计算资源集中起来，并由软件实现自动管理，无须人为参与。这使得应用提供者无须为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。有人打了个比方：这就好比是从古老的单台发电机模式转向了电厂集中供电的模式。它意味着计算能力也可以作为一种商品进行流通，就像煤气、水电一样，取用方便，费用低廉。最大的不同在于，它是通过互联网进行传输的。云计算是并行计算（Parallel Computing）、分布式计算（Distributed Computing）和网格计算（Grid Computing）的发展，是虚拟化（Virtualization）、效用计算（Utility Computing）、IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）等概念混合演进并跃升的结果。云计算是网格计算的商业演化版。

目前，云计算并没有统一的定义，这也与云计算本身特征很相似。维基百科对云计算的定义是：云计算是一种基于互联网的计算新方式，通过互联网上异构、自治的服务为个人和企业提供按需即取的计算。由于资源是在互联网上，而互联网通常以云状图案来表示，因此以云来类比这种计算服务，同时云也是对底层基础设施的一种抽象概念。云计算的资源是动态扩展且虚拟化的，通过互联网提供，终端用户不需要了解云中基础设施的细节，不必具有专业的云技术知识，也无须直接进行控制，只关注自身真正需要什么样的资源以及如何通过网络来获得相应的服务。关于云计算的描述，在当前具有的共同特征是：云是一种服务，类似水电一样，按需使用、灵活付费，使用者只关注服务本身。H3C的云计算理念认为云计算是一种新的IT服务模式，支持大规模计算资源的虚拟化，提供按需计算、动态部署、灵活扩展能力。

3．云计算的服务模式

云计算平台包括如图6-1所示的三种典型服务模式：

软件即服务(Software as a Service)

● 用户通过标准的Web浏览器来使用Internet上的软件。
● 客户端软件通过标准的Web服务来使用Internet上的服务。
● 用户不必购买软件，只需按需租用软件。

平台即服务(Plaform as a Service)

● 提供应用服务引擎，如互联网应用编程接口/运行平台等。
● 用户基于该应用服务引擎，可以构建该类应用。

基础设施即服务(Infrastructure as a Service)

● 以服务的形式提供虚拟硬件资源，如虚拟主机/存储/网络/安全等资源。
● 用于无须购买服务器、网络设备、存储设备，只需要通过互联网租赁即可搭建自己的应用系统。

图 6-1　云计算服务模式

1）基础设施即服务（Infrastructure as a Service，IaaS）

基础设施即服务指的是为用户提供网络、计算和存储一体化的基础架构服务，通过 Iaas 服务，客户端无须购买服务器、软件等网络设备，即可任意部署和使用存储、网络和其他基本的计算资源。在 Iaas 服务中，用户不能控制底层的基础设施，但是可以控制操作系统、存储装置和已部署的应用程序。

在 IaaS 中，一台物理机器往往被划分为多台虚拟机器进行使用。由于同一物理服务器的虚拟机之间可以相互访问，而不需要经过之外的防火墙与交换机等设备，因此虚拟机之间的攻击变得更加容易。另外，服务商提供的是一个共享的基础设施，例如 CPU 缓存、GPU 等，这些基础设施对使用者来说并不是完全隔离的，当一个攻击者得逞时，全部服务器都向攻击者敞开了大门，因此对 Iaas 服务的分区和服务环境监控是云安全中的重要研究领域，如何保证同一物理机上不同虚拟机之间的资源隔离，包括 CPU 调度、内存虚拟化、VLAN、I/O 设备虚拟化之间，是当前 IaaS 服务模式下首要解决的安全技术问题。

2）平台即服务（Platform as a Service，PaaS）

把服务器平台或者开发环境作为一种服务提供的商业模式。PaaS 实际上是指将软件研发的平台作为一种服务，具体可以归类为应用服务器、业务能力接入、业务引擎、企业进行定制化研发的中间件平台等，通过 PaaS 提供的 API 开放给 PaaS 用户。

PaaS 可以提高在 Web 平台上利用的资源数量。例如，可通过远程 Web 服务使用数据即服务（Data-as-a-Service：数据即服务）。用户或者厂商基于 PaaS 平台可以快速开发自己所需要的应用和产品。同时，PaaS 平台开发的应用能更好地搭建基于 SOA 架构的企业应用，如云平台通过提供二次开发接口、软件定制接口等功能以及开放式的支撑服务功能，提供完善的应用服务引擎和应用编程接口，用户能通过应用服务引擎，无须专业程序员，直接在线开发相应的企业应用。

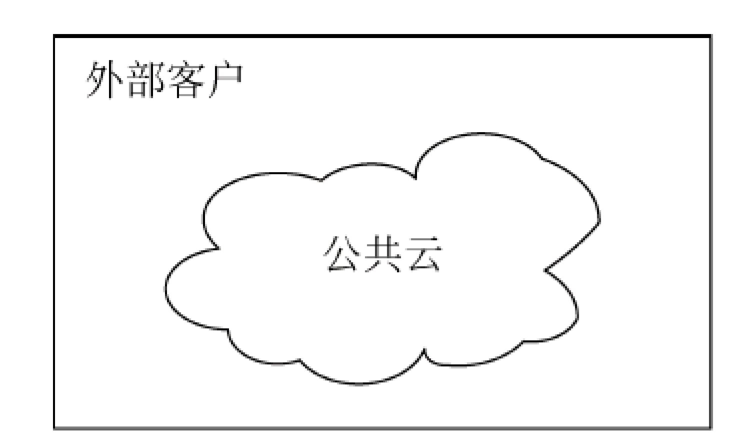
3）软件即服务(Software as a Service,SaaS)

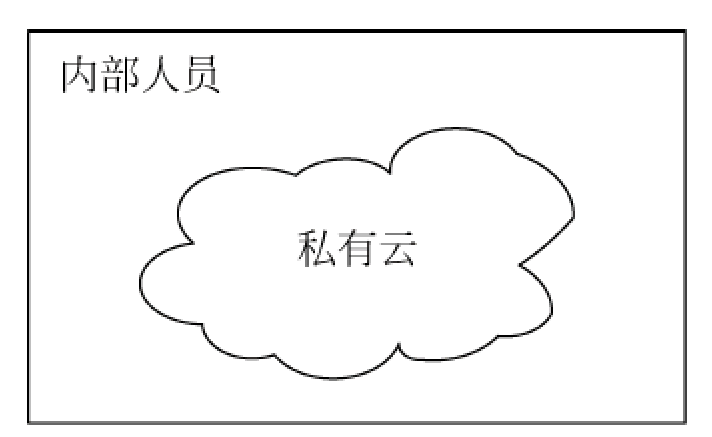
软件即服务与按需软件(on-demand software),应用服务提供商(the application service provider,ASP),托管软件(hosted software)具有相似的含义。它是一种通过Internet提供软件的模式,厂商将应用软件统一部署在自己的服务器上,客户可以根据自己的实际需求,通过互联网向厂商定购所需的应用软件服务,按定购的服务多少和时间长短向厂商支付费用,并通过标准的Web浏览器来使用云平台上的各类在线服务,用户不必购买软件,只须按需租用云平台上的各类正版软件和在线软件服务功能,且无须对软件进行维护,服务提供商会全权管理和维护软件,软件厂商在向客户提供互联网应用的同时,也提供软件的离线操作和本地数据存储,让用户随时随地都可以使用其定购的软件和服务。

对于许多小型企业来说,SaaS是采用先进技术的最好途径,它消除了企业购买、构建和维护基础设施和应用程序的需要,减少了企业运维和购买软件的成本。

4. 云计算部署模式

在部署模式上,云计算有三种模式,如图6-2所示。





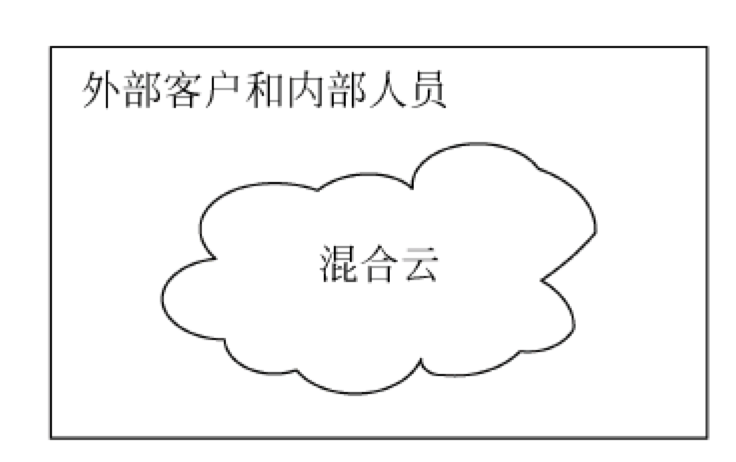


图6-2 云计算的三种部署模式

1）公共云

公共云是指为外部客户提供服务的云,它所有的服务是供别人使用,而不是自己用。目前,典型的公共云有微软的Windows Azure Platform、亚马逊的AWS、Salesforce.com以及国内的阿里巴巴、用友伟库等。对于使用者而言,公共云的最大优点是,其所应用的程序、服务及相关数据都存放在公共云的提供者处,自己无须做相应的投资和建设。目前最大的问题是,由于数据不存储在自己的数据中心,其安全性存在一定风险。同时,公共云的可用性不受使用者控制,这方面也存在一定的不确定性。

2）私有云

私有云是指企业自己使用的云,它所有的服务不是供别人使用,而是供企业自己的内部人员或分支机构使用。私有云的部署比较适合于有众多分支机构的大型企业或政府部门。随着这些大型企业数据中心的集中化,私有云将会成为他们部署IT系统的主流模式。相对于公共云,私有云部署在企业自身内部,因此其数据安全性、系统可用性都可由自己控制。

但其缺点是投资较大,尤其是一次性的建设投资较大。

3) 混合云

混合云是指供自己和客户共同使用的云,它所提供的服务既可以供别人使用,也可以供自己使用。相比较而言,混合云的部署方式对提供者的要求较高。

5. 云计算的发展

云计算从1959年概念的提出到今天的初步成熟,已经经历了几十年的发展历程。

1959年,Christopher Strachey发表虚拟化论文,虚拟化是今天云计算基础架构的基石。

1961年,John McCarthy提出计算力和通过公用事业销售计算机应用的思想。

1962年,J. C. R. Licklier提出"星际计算机网络"设想。

1984年,Sun公司的联合创始人John Gage提出"网络就是计算机"的名言,用于描述分布式计算技术带来的新世界,今天的云计算正在将这一理念变成现实。

1997年,南加州大学教授Ramnath K. Chellappa提出云计算的第一个学术定义,认为计算的边界可以不是技术局限,而是经济合理性。

1998年,VMware(威睿公司)成立并首次引入X86的虚拟技术。

1999年,MarcAnreessen创建LouClou,是第一个商业化的IaaS平台。

2004年,Google发布MapReuce论文。Hadoop就是Google集群系统的一个开源项目总称,主要由HFS、MapReuce和Hbase组成,其中HFS是GoogleFileSystem(GFS)的开源实现;MapReuce是GoogleMapReuce的开源实现;HBase是GoogleBigTable的开源实现。

2005年,Amazon宣布Amazon Web Services云计算平台,并在2006年相继推出在线存储服务S3和弹性计算云EC2等云服务。

2007年,Google与IBM在大学开设云计算课程。戴尔成立数据中心解决方案部门,先后为全球5大云计算平台中的三个(包括Windows Azure、Facebook和Ask. com)提供云基础架构。亚马逊公司推出了简单队列服务(Simple Queue Service,SQS),这项服务使托管主机可以存储计算机之间发送的消息。IBM首次发布云计算商业解决方案,推出"蓝云"(Blue Cloud)计划。

2008年,Salesforce. com推出了随需应变平台evForce, Force. com平台是世界上第一个平台即服务的应用。

2009年,思科发布统一计算系统(UCS)、云计算服务平台,VMWare推出业界首款云操作系统Vmware vSphere 4, Google推出Chrome OS操作系统。

2010年, Microsoft正式发布Microsoft Azure云平台服务。英特尔在IDF上提出互联计算,用X86架构统一嵌入式、物联网和云计算领域。戴尔推出源于DCS部门设计的PowerEdgeC系列云计算服务器及相关服务。

在我国,云计算的发展也颇为迅猛。

2008年3月17日,Google全球CEO埃里克·施密特(Eric Schmidt)在北京访问期间,宣布在中国大陆推出"云计算(Cloud Computing)"计划。而2008年初,IBM与无锡市政府合作建立了无锡软件园云计算中心,开始了云计算在中国的商业应用。2008年7月份瑞星推出了"云安全"计划。

2009年,VMware在中国召开的vForum用户大会,第一次将开放云计算的概念带入中国。

2010年10月18日发布《国务院关于加快培育和发展战略性新兴产业的决定》中,将云计算定位于"十二五"战略性新兴产业之一。同一天,工信部、发改委联合印发《关于做好云计算服务创新发展试点示范工作的通知》,确定在北京、上海、深圳、杭州、无锡等五个城市先行开展云计算服务创新发展试点示范工作,让国内的云计算热潮率先从政府云开始熊熊燃烧。

云计算在中国有着巨大的市场潜力,不仅仅在于中国幅员辽阔,人口众多。更重要的是中国从2009年已经成为全球最大的PC消费国,也会成为最大的PC服务器拥有国。庞大的IT投资也成为国家节能减排中值得重点关注的一环,云计算将成为绿色IT、节能减排最为重要的手段,提高了IT灵活性和可持续发展,也将积极推动和谐社会的构建,这也是为什么政府在"十二五"规划中将云计算定位为战略性新兴产业的原因之一。

云计算作为一种应用模式,它的出现和应用范围日益扩大,必将对产业链的上下游产生重要影响,它在不断地适应着企业的需求。未来云计算的发展,将朝着平台化、公共云和混合云、大数据等方向发展,未来的云计算将更强调安全性和性能,云游戏的领域也将会是云的另一个主要的发展趋势。

6. 云计算平台简介

目前,比较优秀的云计算平台主要包括Google云计算平台、IBM"蓝云"云计算平台、Amazon的弹性计算云、微软的云计算架构等。

1) Google云计算平台

Google云计算平台是全球最大的搜索引擎,包括Google Maps、Google Earth、Gmail、YouTube等一系列产品,这个平台最初是为Google最重要的搜索应用提供服务,现在已经扩展到其他应用领域,其特点是数据量庞大、面向全球用户提供实时服务。

Google的硬件条件优势、大型的数据中心和搜索引擎的支柱应用,促进Google云计算迅速发展。Google的云计算基础架构模式包括4个相互独立又紧密结合在一起的系统:Google File System分布式文件系统,针对Google应用程序的特点提出的MapReduce编程模式,分布式的锁机制Chubby以及Google开发的模型简化的大规模分布式数据库BigTable。

Google File System文件系统(GFS):除了性能,可伸缩性、可靠性以及可用性以外,GFS设计还受到Google应用负载和技术环境的影响。体现在4个方面:

(1) 充分考虑到大量节点的失效问题,需要通过软件将容错以及自动恢复功能集成在系统中;

(2) 构造特殊的文件系统参数,文件通常大小以G字节计,并包含大量小文件;

(3) 充分考虑应用的特性,增加文件追加操作,优化顺序读写速度;

(4) 文件系统的某些具体操作不再透明,需要应用程序的协助完成。

如图6-3所示,给出了Google File System的系统架构。

一个GFS集群包含一个主服务器和多个块服务器,被多个客户端访问。文件被分割成固定尺寸的块。在每个块创建的时候,服务器分配给它一个不变的、全球唯一的64位块句

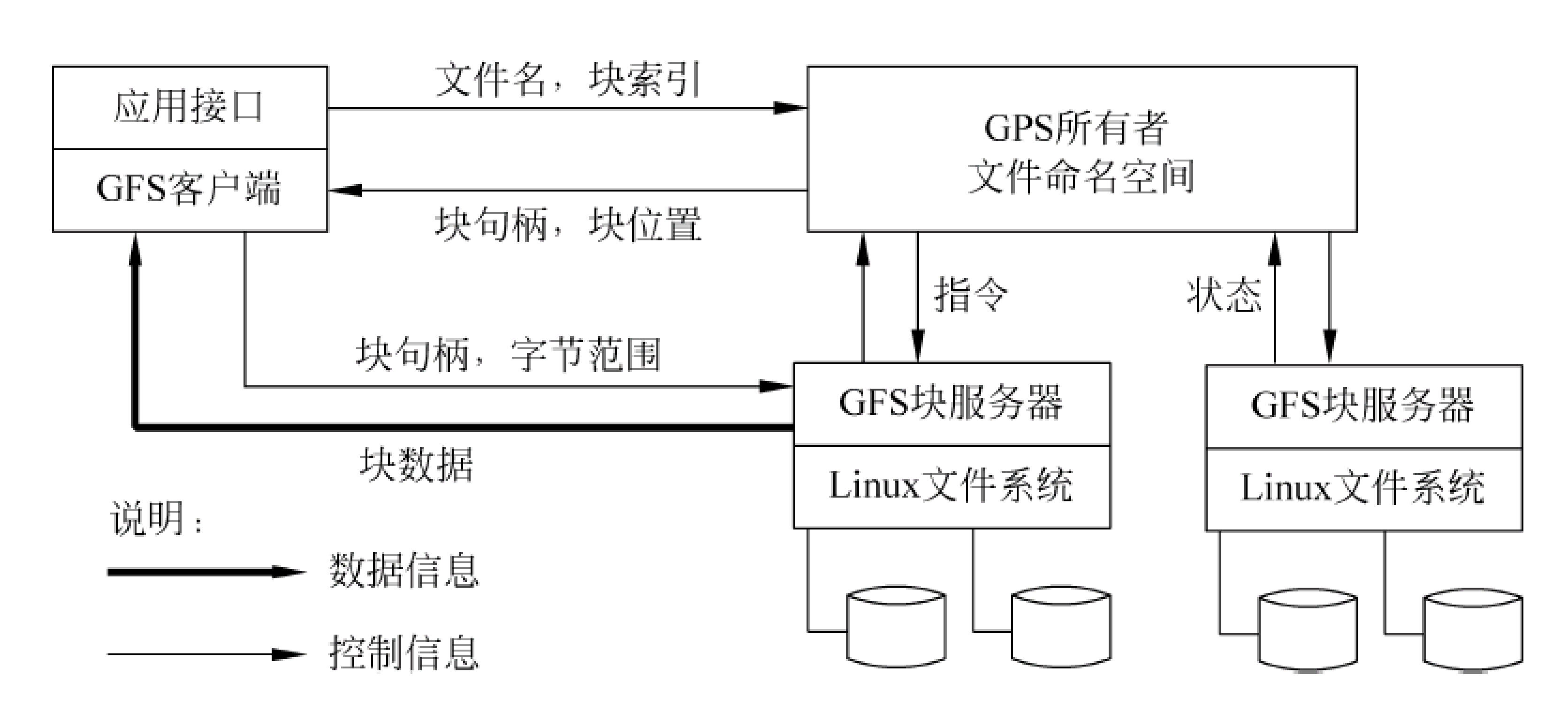


图 6-3　Google File System

柄对它进行标识。块服务器把块作为 linux 文件保存在本地硬盘上，并根据指定的块句柄和字节范围来读写块数据。为了保证可靠性，每个块都会复制到多个块服务器上，默认保存三个备份。主服务器管理文件系统所有的元数据，包括名字空间、访问控制信息和文件到块的映射信息，以及块当前所在的位置。GFS 客户端代码被嵌入到每个程序里，它实现了 Google 文件系统 API，帮助应用程序与主服务器和块服务器通信，对数据进行读写。客户端跟主服务器交互进行元数据操作，但是所有的数据操作的通信都是直接和块服务器进行的。客户端提供的访问接口类似于 POSIX 接口，但有一定的修改，并不完全兼容 POSIX 标准。通过服务器端和客户端的联合设计，Google File System 能够针对它本身的应用获得最大的性能以及可用性效果。

Map Reduce 分布式编程环境：Google 构造 Map Reduce 编程规范来简化分布式系统的编程，应用程序编写人员只需将精力放在应用程序本身。而关于集群的处理问题，包括可靠性和可扩展性，则交由平台来处理。Map Reduce 通过映射(Map)和化简(Reduce)这样两个简单的概念来构成运算基本单元，用户只需提供自己的 Map 函数以及 Reduce 函数即可并行处理海量数据。

分布式的大规模数据库管理系统 Big Table：由于一部分 Google 应用程序需要处理大量的格式化以及半格式化数据，Google 构建了弱一致性要求的大规模数据库系统 Big Table。Big Table 的应用包括 Search History、Maps、Orkut、RSS 阅读器等。

Big Table 是客户端和服务器端的联合设计，使得性能能够最大程度地符合应用的需求。Big Table 系统依赖于集群系统的底层结构。一个是分布式的集群任务调度器，一个是前述的 Google 文件系统，还有一个分布式的锁服务 Chubby。

Chubby 是一个非常鲁棒的粗粒度锁，Big Table 使用 Chubby 来保存根数据表格的指针，即用户可以首先从 Chubby 锁服务器中获得根表的位置，进而对数据进行访问。Big Table 使用一台服务器作为主服务器，用来保存和操作元数据。主服务器除了管理元数据之外，还负责对 Table 服务器(即一般意义上的数据服务器)进行远程管理与负载调配。客户端通过编程接口与主服务器进行元数据通信，与 Table 服务器进行数据通信。

2）IBM“蓝云”云计算平台

“蓝云”解决方案是由 IBM 云计算中心开发的企业级云计算解决方案。该解决方案可以对企业现有的基础架构进行整合，通过虚拟化技术和自动化技术，构建企业自己拥有的云

计算中心,实现企业硬件资源和软件资源的统一管理、统一分配、统一部署、统一监控和统一备份,打破应用对资源的独占,从而帮助企业实现云计算理念。

IBM 的“蓝云”计算平台是一套完整的软、硬件平台,将 Internet 上使用的技术扩展到企业平台上,使得数据中心使用类似于互联网的计算环境。“蓝云”大量使用了 IBM 先进的大规模计算技术,结合了 IBM 自身的软、硬件系统以及服务技术,支持开放标准与开放源代码软件。

“蓝云”基于 IBM Almaden 研究中心的云基础架构,采用了 Xen 和 PowerVM 虚拟化软件,Linux 操作系统映像以及 Hadoop 软件(Google File System 以及 Map Reduce 的开源实现)。IBM 已经正式推出了基于 x86 芯片服务器系统的“蓝云”产品。

“蓝云”计算平台由一个数据中心、IBM Tivoli 部署管理软件(Tivoli provisioning manager)、IBM Tivoli 监控软件(IBM Tivoli monitoring)、IBM WebSphere 应用服务器、IBM DB2 数据库以及一些开源信息处理软件和开源虚拟化软件共同组成。“蓝云”的硬件平台环境与一般的 x86 服务器集群类似,使用刀片的方式增加了计算密度。“蓝云”软件平台的特点主要体现在虚拟机以及对于大规模数据处理软件 Apache Hadoop 的使用上。

“蓝云”平台的一个重要特点是虚拟化技术的使用。虚拟化的方式在“蓝云”中有两个级别,一个是在硬件级别上实现虚拟化,另一个是通过开源软件实现虚拟化。硬件级别的虚拟化可以使用 IBM p 系列的服务器,获得硬件的逻辑分区 LPAR(logic partition)。逻辑分区的 CPU 资源能够通过 IBM Enterprise Workload Manager 来管理。通过这样的方式加上在实际使用过程中的资源分配策略,能够使相应的资源合理地分配到各个逻辑分区。p 系列系统的逻辑分区最小粒度是 1/10 颗 CPU。Xen 则是软件级别上的虚拟化,能够在 Linux 基础上运行另外一个操作系统。

3) Amazon 的弹性计算云

亚马逊是互联网上最大的在线零售商,但是同时也为独立开发人员以及开发商提供云计算服务平台。亚马逊将他们的云计算平台称为弹性计算云(Elastic Compute Cloud, EC2),它是最早提供远程云计算平台服务的公司。

与 Google 提供的云计算服务不同,Google 仅为自己在互联网上的应用提供云计算平台,独立开发商或者开发人员无法在这个平台上工作,因此只能转而通过开源的 Hadoop 软件支持来开发云计算应用。亚马逊的弹性计算云服务也和 IBM 的云计算服务平台不一样,亚马逊不销售物理的云计算服务平台,没有类似于“蓝云”一样的计算平台。亚马逊将自己的弹性计算云建立在公司内部的大规模集群计算的平台之上,而用户可以通过弹性计算云的网络界面去操作在云计算平台上运行的各个实例(Instance),付费方式则由用户的使用状况决定,即用户仅需要为自己所使用的计算平台实例付费,运行结束后计费也随之结束。

弹性计算云从严格上来看,并不是亚马逊公司推出的第一项这种服务,它由名为亚马逊网络服务的现有平台发展而来。早在 2006 年 3 月,亚马逊就已经发布了简单存储服务(Simple Storage Service, S3),这种存储服务按照每个月类似租金的形式进行服务付费,同时用户还需要为相应的网络流量进行付费。亚马逊网络服务平台使用 REST(Representational State Transfer)和简单对象访问协议(SOAP)等标准接口,用户可以通过这些接口访问到相应的存储服务。

2007 年 7 月,亚马逊公司推出了简单队列服务(Simple Queue Service, SQS),这项服务

使托管主机可以存储计算机之间发送的消息。通过这一项服务，应用程序编写人员可以在分布式程序之间进行数据传递，而无须考虑消息丢失的问题。通过这种服务方式，即使消息的接收方还没有模块启动也没有关系。服务内部会缓存相应的消息，而一旦有消息接收组件被启动运行，则队列服务将消息提交给相应的运行模块进行处理。同样的，用户必须为这种消息传递服务进行付费使用，计费的规则与存储计费规则类似，依据消息的个数以及消息传递的大小进行收费。

4）微软的云计算架构

微软最新发布的服务器和云平台网站已经可以提供包括管理云应用、部署服务器等多种功能在内的一站式云服务。

除了可为消费者构建私有云外，该网站还提供虚拟服务器、虚拟桌面、管理云应用、部署服务器、管理员身份认证、数据分析等服务。

此外，用户还可以从该网站浏览新闻、查看微软最新产品、公告等，实现量身定制的个性上网方案。

基于如图 6-4 所示的架构，微软为企业提供两种云计算部署类型，即公共云和私有云。

公共云：由微软自己运营，为客户提供部署和应用服务。在公共云中，Windows Azure Platform 是一个高度可扩展的服务平台，提供基于微软数据中心随用随付费的灵活的服务模式。

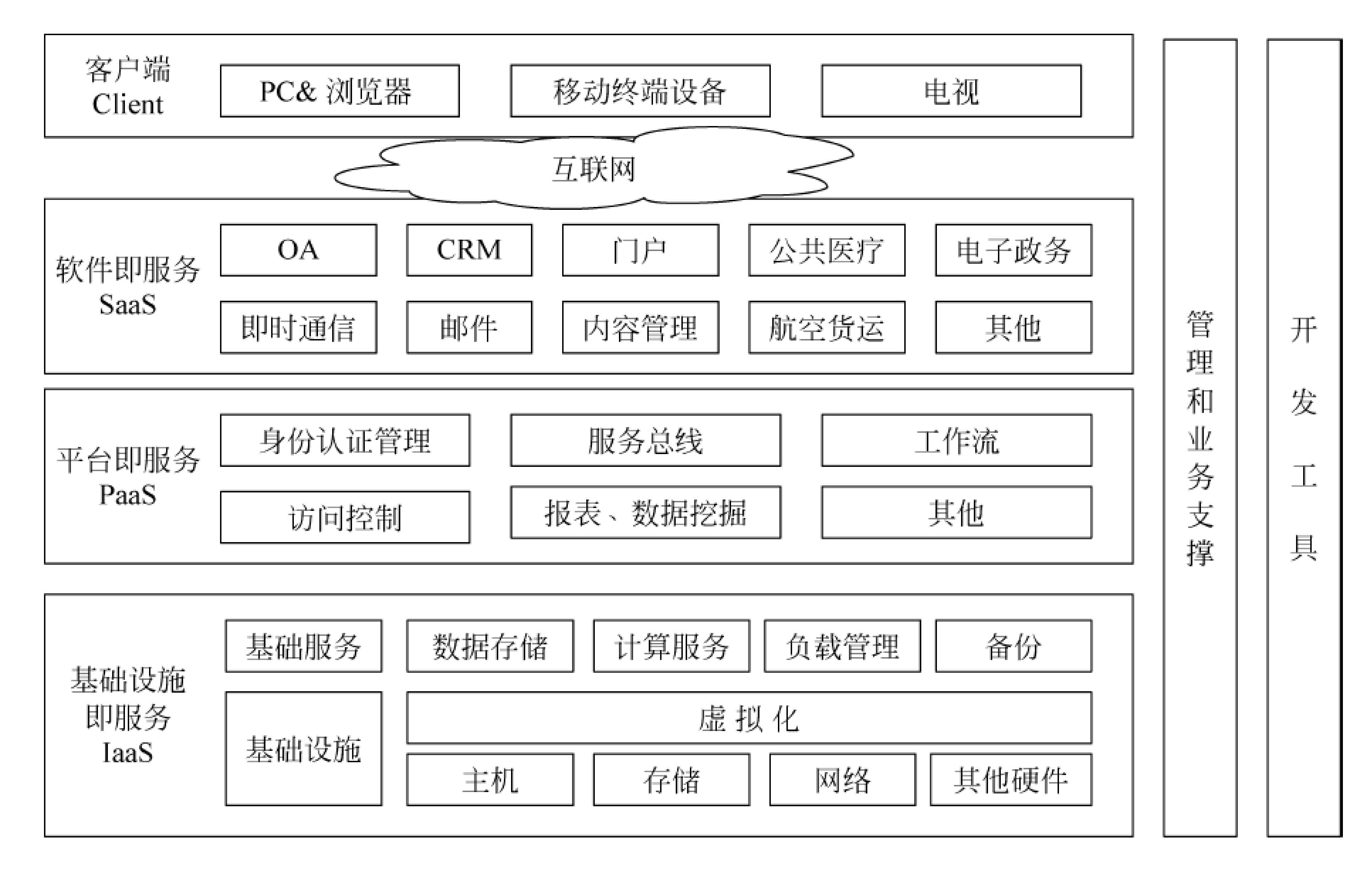


图 6-4 微软云计算架构图

私有云：部署在客户的数据中心内部，基于客户个性化的性能和成本要求、面向服务的内部应用环境。这个云平台基于成熟的 Windows Server 和 System Center 等系列产品，并且能够与现有应用程序兼容。

有鉴于云计算如火如荼的快速发展，微软几乎针对全线产品都提出了明确的云战略，其云计算解决方案包括公共云和私有云，既可以帮助企业搭建私有云，又可以帮助企业构建公

共云，或让企业选择基于微软云平台运营企业的公共云服务。微软为自己的客户和合作伙伴提供三种不同的云计算运营模式。

公有云：微软自己构建及运营公共云的应用和服务，同时向个人消费者和企业客户提供云服务。

合作伙伴运营：独立软件开发商或系统集成商等各种合作伙伴可基于微软 Windows Azure Platform 开发 ERP、CRM 等各种云计算应用，并在这一平台上为最终使用者提供服务。

客户自建私有云：客户可以选择微软的云计算解决方案构建自己的云计算平台。微软可以为用户提供包括产品、技术、平台和运维管理在内的全面支持。

微软云战略包括三大部分，为客户和合作伙伴提供三种不同的云计算运营模式。

(1) 微软运营：微软自己构建及运营公共云的应用和服务，同时向个人消费者和企业客户提供云服务。例如，微软向最终使用者提供的 Online Services 和 Windows Live 等服务。

(2) 伙伴运营：ISV/SI 等各种合作伙伴可基于 Windows Azure Platform 开发 ERP、CRM 等各种云计算应用，并在 Windows Azure Platform 上为最终使用者提供服务。另外一个选择是，微软运营在自己的云计算平台中的 Business Productivity Online Suite (BPOS) 产品也可交由合作伙伴进行托管运营。BPOS 主要包括 Exchange Online，SharePoint Online，Office Communications Online 和 LiveMeeting Online 等服务。

(3) 客户自建：客户可以选择微软的云计算解决方案构建自己的云计算平台。微软可以为用户提供包括产品、技术、平台和运营管理在内的全面支持。在云计算时代，一个企业是否可以不用部署任何的 IT 系统，一切都从云计算平台获取，或者反过来，企业还是像以前一样，全部的 IT 系统都部署在企业内部，不从云中获取任何的服务。

很多企业认为有些 IT 服务适合从云中获取，如 CRM、网络会议、电子邮件等；但有些系统不适合部署在云中，如自己的核心业务系统、财务系统等。因此，微软认为理想的模式将是“软件＋服务”，即企业既会从云中获取必需的服务，也会自己部署相关的 IT 系统。如图 6-5 所示是微软的“软件＋服务”战略。

“软件＋服务”可以简单地描述为两种模式：

(1) 软件本身架构模式是“软件加服务”。例如，杀毒软件本身部署在企业内部，但是杀毒软件的病毒库更新服务是通过互联网进行的，即从云中获取。

(2) 企业的一些 IT 系统由自己构建，另一部分向第三方租赁，从云中获取服务。例如，企业可以直接购买软硬件产品，在企业内部自己部署 ERP 系统，而同时通过第三方云计算平台获取 CRM、电子邮件等服务，而不是自己建设相应的 CRM 和电子邮件系统。

“软件＋服务”的好处在于，既充分继承了传统软件部署方式的优越性，又大量利用了云计算的新特性。

在云计算时代，有三个平台非常重要，即开发平台、部署平台和运营平台。Windows Azure Platform 是微软的云计算平台，其在微软的整体云计算解决方案中发挥关键作用。它既是运营平台，又是开发、部署平台；上面既可运行微软的自有应用，也可以开发部署用户或 ISV 的个性化服务；平台既可以作为 SaaS 等云服务的应用模式的基础，又可以与微软线下的系列软件产品相互整合和支撑。事实上，微软基于 Windows Azure Platform，在云

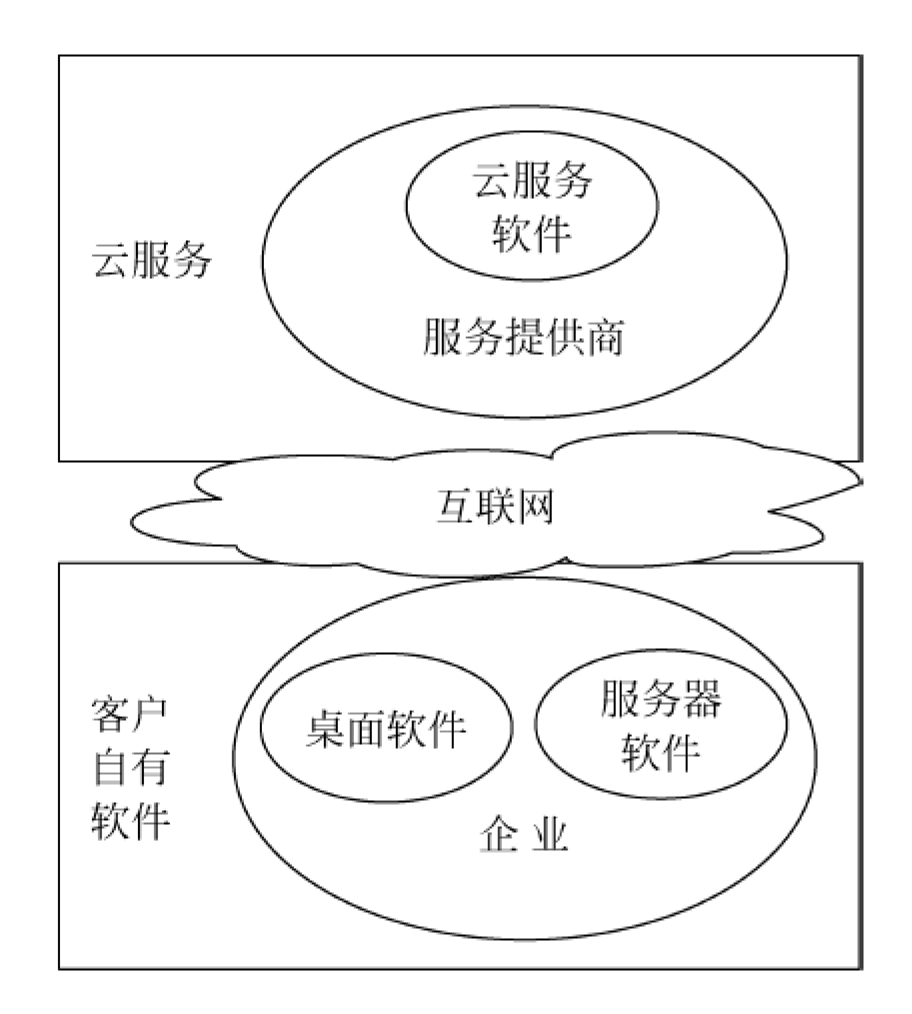


图 6-5　微软的"软件＋服务"战略

计算服务和线下客户自有软件应用方面都拥有了更多样化的应用交付模式、更丰富的应用解决方案、更灵活的产品服务部署方式和商业运营模式。

企业可以根据自身的具体需求和特征，微软为用户提供自由选择的机会。

为用户提供自由选择的机会是微软云计算战略的第三大典型特点。这种自由选择表现在以下三个方面：

（1）用户可以自由选择传统软件或云服务两种方式。

自己部署 IT 软件、采用云服务、或者两者都用，无论是用户选择哪种方式，微软的云计算都能支持。

（2）用户可以选择微软不同的云服务。

无论用户需要的是 SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）还是 IaaS（Infrastructure-as-a-Service），微软都有丰富的服务供其选择。微软拥有全面的 SaaS 服务，包括针对消费者的 Live 服务和针对企业的 Online 服务；也提供基于 Windows Azure Platform 的 PaaS 服务；还提供数据存储、计算等 IaaS 服务和数据中心优化服务。用户可以基于任何一种服务模型选择使用云计算的相关技术、产品和服务。

（3）用户和合作伙伴可以选择不同的云计算运营模式。

微软提供多种云计算运营模式。用户和合作伙伴可直接应用微软运营的云计算服务；用户也可以采用微软的云计算解决方案和技术工具自建云计算应用；合作伙伴还可以选择运营微软的云计算服务或自己在微软云平台上开发云计算应用。

6.1.2　云计算核心技术

云计算系统运用了许多技术，其中以编程模型、数据管理技术、数据存储技术、虚拟化技术、云计算平台管理技术最为关键。

1. 编程模型

Map Reduce 是一种编程模型，用于大规模数据集（大于 1TB）的并行运算。映射（Map）

和归约(Reduce)的主要思想,都是从函数式编程语言里借来的,还有从矢量编程语言里借来的特性。它极大地方便了编程人员在不会分布式并行编程的情况下,将自己的程序运行在分布式系统上。当前的软件实现是指定一个映射(Map)函数,用来把一组键值对映射成一组新的键值对,指定并发的归约(Reduce)函数,用来保证所有映射的键值对中的每一个共享相同的键组。

Map Reduce 是 Google 开发的 java、Python、C++ 编程模型,它是一种简化的分布式编程模型和高效的任务调度模型,用于大规模数据集(大于 1TB)的并行运算。严格的编程模型使云计算环境下的编程十分简单。Map Reduce 模式的思想是将要执行的问题分解成映射(Map)和归纳(Reduce)的方式,先通过 Map 程序将数据切割成不相关的区块,分配(调度)给大量计算机处理,达到分布式运算的效果,再通过 Reduce 程序将结果汇整输出。

Map Reduce 编程模型结合用户实现的 Map 和 Reduce 函数,可完成大规模的并行化计算。Map Reduce 编程通过用户自定义的 Map 函数处理一个输入的基于 key/value 对的集合,输出中间基于 key/value 对的集合,Map Reduce 库把中间所有具有相同 key 值的 value 值集合在一起后传递给 Reduce 函数,用户自定义的 Reduce 函数合并所有具有相同 key 值的 value 值,形成一个较小 value 值的集合。典型的 Map Reduce 程序的执行步骤如下所示:

(1) 有多个 Map 任务,每个任务的输入为 DFS 中的一个或者多个文件块。Map 将文件块转换为一个 Key-Value 对序列,而此处的逻辑就是 Mapper 的业务算法。

(2) 主控制器(master controller),从每个 Map 任务中收集一系列键值对,并将它们按照键大小排序,而这些键值再次被分割,然后分配给所有的 Reduce 任务中,相同键值的对集合会被分配到同一个 Reduce 任务。该部分就是 Map Reduce 和核心 Shuffle 的任务。在 Mapper 端结果进行:分区、排序、分割。在 Reduce 端将 Map 的结果分割后的任务派发给 Reduce,最核心的就是 merge 过程。

(3) Reduce 任务每次作用于一个键,并将与此键关联的所有值以某种方式组合起来。具体的组合方式取决于用户所编写的 Reduce 函数代码。

如图 6-6 所示,Hadoop 任务被分解为几个节点,而 Map Reduce 任务则被分解为跟踪器(tracker)。

如图 6-7 所示,显示了 Map Reduce 如何执行任务,它将获取输入并执行一系列分组、排序和合并操作,然后呈现经过排序和散列的输出。

图 6-7 演示了一个更复杂的 Map Reduce 任务及其组成部分。用户提交一个任务以后,该任务由 Job Tracker 协调,先执行 Map 阶段,然后执行 Reduce 阶段。Map 阶段和 Reduce 阶段动作都受到 Task Tracker 监控,并运行在独立于 Task Tracker 的 Java 虚拟机中。

输入和输出都是 HDFS 上的目录。输入由 Input Format 接口描述,它的实现如 ASCII 文件,JDBC 数据库等,分别处理对应的数据源,并提供了数据的一些特征。通过 Input Format 实现,可以获取 Input Split 接口的实现,这个实现用于对数据进行划分(图中的 splite1 到 splite5,就是划分以后的结果),同时从 Input Format 也可以获取 Record Reader 接口的实现,并从输入中生成＜k,v＞对。有了＜k,v＞,就可以开始做 Map 操作了。

Map 操作通过 context. collect(最终通过 OutputCollector. collect)将结果写到 context 中。当 Mapper 的输出被收集后,它们会被 Partitioner 类以指定的方式区分地写出到输出

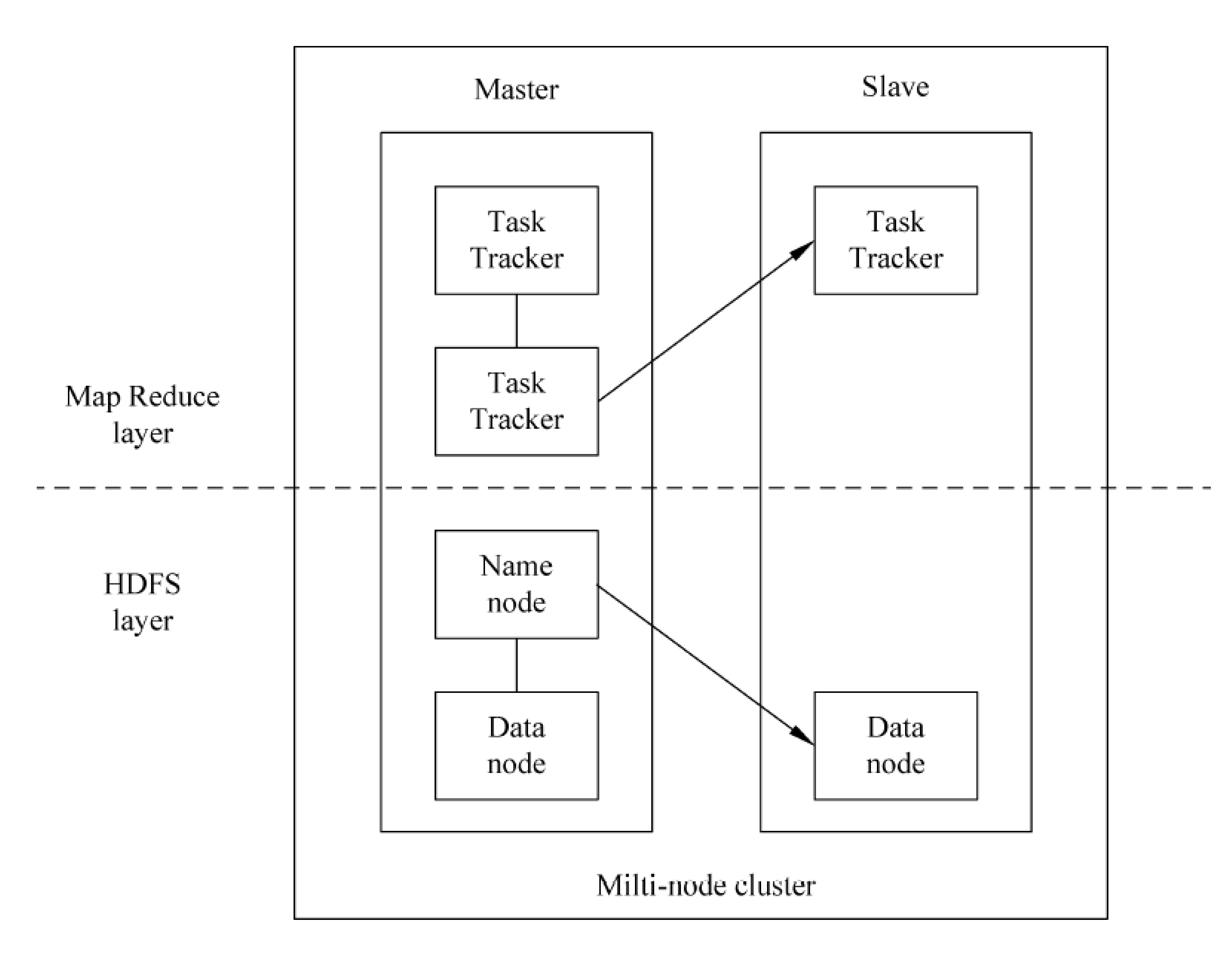


图 6-6 HDFS/Map Reduce 层的组成部分

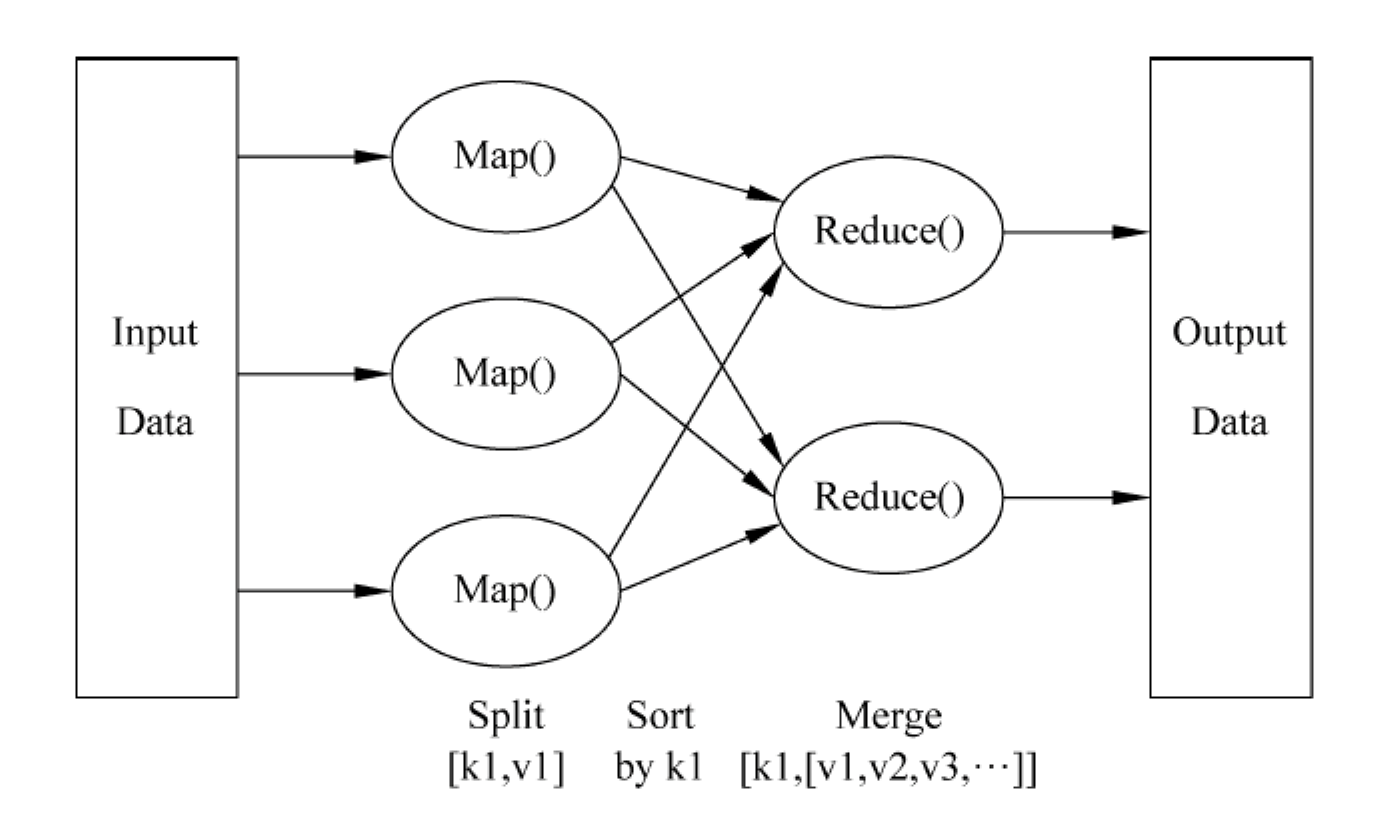


图 6-7 Map Reduce 执行任务图

文件里。我们可以为 Mapper 提供 Combiner，在 Mapper 输出它的<k,v>时，键值对不会被马上写到输出里，他们会被收集在 list 里（一个 key 值一个 list），当写入一定数量的键值对时，这部分缓冲会被 Combiner 中进行合并，然后再输出到 Partitioner 中（图中 M1 的深色阴影部分对应着 Combiner 和 Partitioner）。

Map 的动作做完以后，进入 Reduce 阶段。这个阶段分 3 个步骤：混洗（Shuffle）、排序（Sort）和归约（Reduce）。

混洗阶段，Hadoop 的 Map Reduce 框架会根据 Map 结果中的 key，将相关的结果传输到某一个 Reducer 上（多个 Mapper 产生的同一个 key 的中间结果分布在不同的机器上，这一步结束后，他们传输都到了处理这个 key 的 Reducer 的机器上）。这个步骤中的文件传输使用了 HTTP 协议。

排序和混洗是一块进行的，这个阶段将来自不同 Mapper 具有相同 key 值的<key，value>对合并到一起。

Reduce 阶段，上面通过 Shuffle 和 Sort 后得到的<key，(list="" of="" values)="">会送到 Reducer. Reduce 方法中处理，输出的结果通过 OutputFormat，输出到 DFS 中。

Map Reduce 数据流图解如图 6-8 所示。

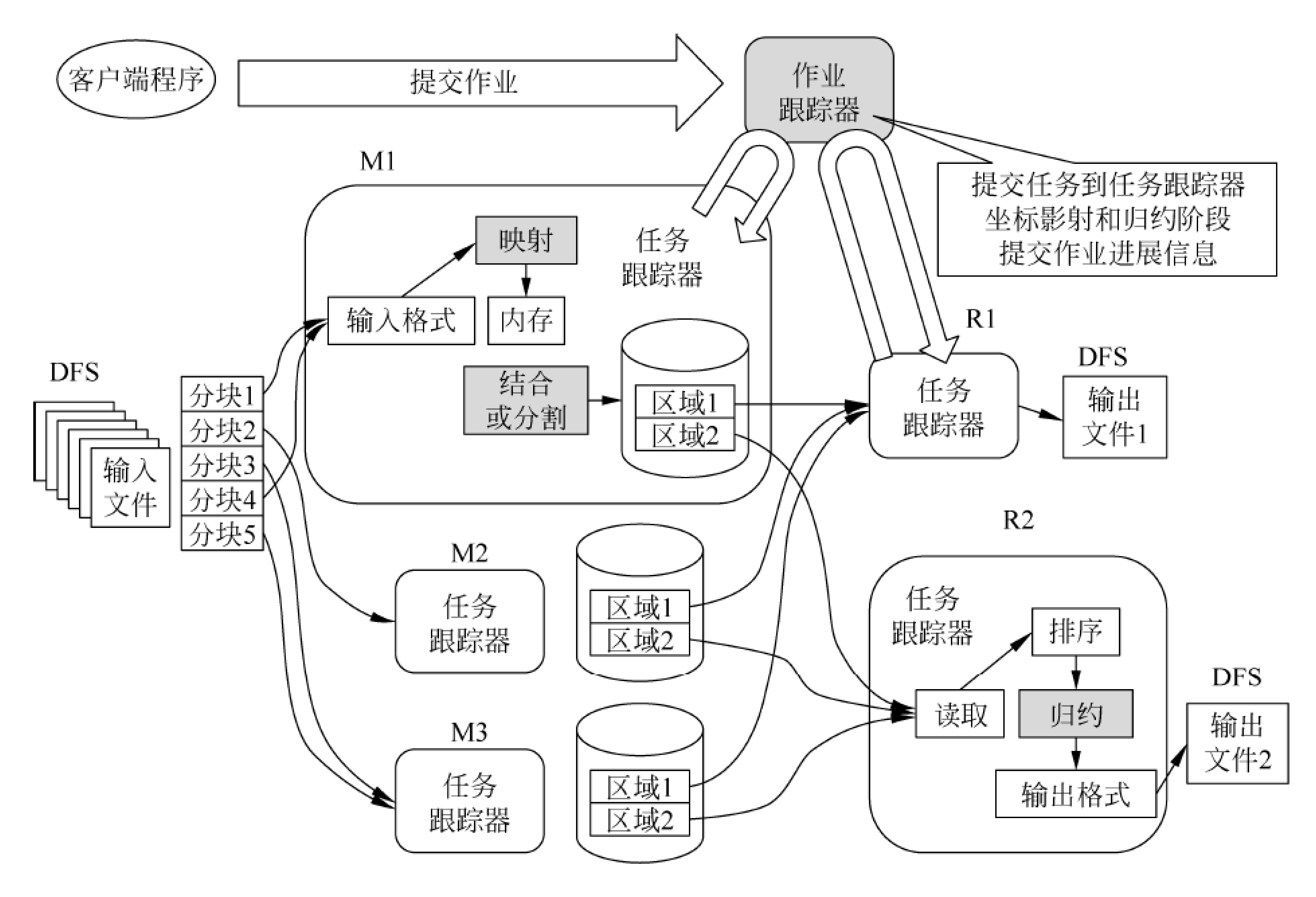


图 6-8 Map Reduce 数据流图解

尽管 Hadoop+Map Reduce 要比传统的分析环境(如 IBM Cognos 和 Satori proCube 在线分析处理)更复杂一些，但它的部署仍然具有可扩展能力和高成本效益。

2. 海量数据分布存储技术

云计算系统由大量服务器组成，同时为大量用户服务，因此云计算系统采用分布式存储的方式存储数据，用冗余存储的方式保证数据的可靠性。云计算系统中广泛使用的数据存储系统是 Google 的 GFS 和 Hadoop 团队开发的 GFS 的开源实现 HDFS。

GFS 即 Google 文件系统(Google File System)，是一个可扩展的分布式文件系统，用于大型的、分布式的、对大量数据进行访问的应用。GFS 的设计思想不同于传统的文件系统，是针对大规模数据处理和 Google 应用特性而设计的。它运行于廉价的普通硬件上，但可以提供容错功能。它可以给大量的用户提供总体性能较高的服务。

一个 GFS 集群由一个主服务器(master)和大量的块服务器(Chunk Server)构成，并被许多客户(Client)访问。主服务器存储文件系统所有的元数据，包括名字空间、访问控制信息、从文件到块的映射以及块的当前位置。它也控制系统范围的活动，如块租约(lease)管理，孤立块的垃圾收集，块服务器间的块迁移。主服务器定期通过 Heart Beat 消息与每一个块服务器通信，给块服务器传递指令并收集它的状态。GFS 中的文件被切分为 64MB 的

块并以冗余存储,每份数据在系统中保存3个以上备份。

客户与主服务器的交换只限于对元数据的操作,所有数据方面的通信都直接和块服务器联系,这大大提高了系统的效率,防止主服务器负载过重。

3. 海量数据管理技术

云计算需要对分布的、海量的数据进行处理、分析,因此,数据管理技术必需能够高效的管理大量的数据。云计算系统中的数据管理技术主要是Google的BT(Big Table)数据管理技术和Hadoop团队开发的开源数据管理模块HBase。

BT是建立在GFS、Scheduler、Lock Service和Map Reduce之上的一个大型的分布式数据库,与传统的关系数据库不同,它把所有数据都作为对象来处理,形成一个巨大的表格,用来分布存储大规模结构化数据。

Google的很多项目使用BT来存储数据,包括网页查询、Google earth和Google金融。这些应用程序对BT的要求各不相同,数据大小(从URL到网页到卫星图像)不同,反应速度不同(从后端的大批处理到实时数据服务)。对于不同的要求,BT都成功地提供了灵活高效的服务。

4. 虚拟化技术

通过虚拟化技术可实现软件应用与底层硬件相隔离,它包括将单个资源划分成多个虚拟资源的裂分模式,也包括将多个资源整合成一个虚拟资源的聚合模式。虚拟化技术根据对象可分成存储虚拟化、计算虚拟化、网络虚拟化等,计算虚拟化又分为系统级虚拟化、应用级虚拟化和桌面虚拟化。

5. 云计算平台管理技术

云计算资源规模庞大,服务器数量众多并分布在不同的地点,同时运行着数百种应用,如何有效地管理这些服务器,保证整个系统提供不间断的服务是巨大的挑战。

云计算系统的平台管理技术能够使大量的服务器协同工作,方便地进行业务部署和开通,快速发现和恢复系统故障,通过自动化、智能化的手段实现大规模系统的可靠运营。

6.1.3 云计算安全威胁

在云计算出现之后,云计算就与安全有着密切的联系,云安全指的是针对云计算自身存在的安全隐患,研究相应的安全防护措施和解决方案,如云计算安全体系架构、云计算应用服务安全、云计算环境的数据保护等,云计算安全是云计算健康可持续发展的重要前提。

1. 云计算安全事故实例

云计算系统的可靠性、性能以及其他技术问题都会带来云计算的相关风险。而且云计算在安全性和风险管理方面仍有不足,即便是最出色的云服务供应商也会遭遇服务中断或速度变慢的问题。

(1) 2009年2月24日,谷歌的Gmail电子邮箱爆发全球性故障,服务中断时间长达4小时。

(2) 2009 年 3 月 17 日，微软的云计算平台 Azure 停止运行约 22 个小时。Azure 平台的宕机可能引发微软客户对该云计算机服务平台的安全担忧，也暴露了云计算的一个巨大隐患。

(3) 2009 年 6 月，Rackspace 遭受了严重的云服务中断故障。供电设备跳闸，备份发电机失效，不少机架上服务器停机。这场事故造成了严重的后果。

(4) 2010 年 1 月，几乎 6 万 8 千名的 Salesforce.com 用户经历了至少 1 个小时的宕机。

(5) 2011 年 4 月 21 日凌晨，亚马逊公司在北弗吉尼亚州的云计算中心宕机，导致包括回答服务 Quora、新闻服务 Reddit、Hootsuite 和位置跟踪服务 FourSquare 在内的一些网站受到了影响。

以上安全事故使得人们进一步思考公有云面临的安全问题。

2. 云计算安全的特征

由于云计算资源虚拟化、服务化的特有属性，与传统安全相比，云计算安全具有一些新的特征。

(1) 传统的安全边界消失，在传统安全中，通过在物理上逻辑上划分安全域，可以清楚地定义边界，但是由于云计算采用虚拟化技术以及多租户模式，传统的物理边界被打破，物理安全边界的防护机制难以在云计算环境中得到有效应用。

(2) 动态性，在云计算环境中，用户的数量和分类不同化频率高，具有动态性和移动性强的特点，其安全防护也要进行相应的动态调整。

(3) 服务安全保障，云计算采用服务的交互模式，涉及服务的设计、开发和交付，需要对服务的全生命周期进行保障服务的可用性和机密性。

(4) 数据安全保护，在云计算中数据不在当地存储，数据私密性、数据完整性保护、数据恢复等数据安全保护手段对于数据的私密性和安全性更加重要。

(5) 第三方监管和审计，由于云计算的模式，使得服务提供商的权利巨大，导致用户的权利可能难以保证，如何确保维护两者之间平衡，需要有第三方监管和审计。

3. 云计算安全核心技术

云计算安全的核心技术包括以下五个方面：

1) 云计算安全面临的威胁

2013 年，云安全联盟(CSA)对云计算的威胁进行了排名，以下是 2013 年几个最严重的云计算安全威胁因素。

(1) 数据泄露。

数据泄露其实每天都在发生，但云计算加重了这种威胁。一个设计不当的多租户云服务数据库将使攻击者不仅仅进入一个账户，而且会进入每一个与该服务相关的其他账户。

(2) 数据丢失。

设备被损坏、意外删除、天灾不可抗力等都会造成永久性的数据丢失，除非供应商提供备份。如果一个企业的数据在上传到云之前就进行加密，就能更好地保护加密密钥或数据。

(3) 账户或服务流量劫持。

黑客通过网络钓鱼、欺诈或利用软件漏洞来劫持无辜的用户。通常黑客根据一个密码

就可以窃取用户多个服务中的资料，因为用户不会为每个服务设立一个不一样的密码。对于供应商，如果被盗的密码可以登录云，那么用户的数据将被窃听、篡改，黑客将向用户返回虚假信息，或重定向用户的服务到欺诈网站。对用户将可能造成严重的损失。

（4）拒绝服务。

剥夺用户访问他们的资源和数据的权利，并造成延迟是破坏云服务的一种攻击方法，这样可能意味着在线服务的死亡。其他形式的攻击，如非对称应用级的 DoS 攻击，在不消耗大量的资源的情况下就可利用弱点将 Web 服务器、数据库和其他云资源作为目标。

（5）恶意的内部人员。

恶意的内部人员风险是每个组织必须考虑的方面。这种情况不一定发生，但当它发生时，它造成的伤害就会很大。云计算安全专家指出，完全依赖于云服务提供商的安全系统，是最大的风险。

2）身份与权限控制

身份与权限控制解决方案是云安全的核心问题之一，在虚拟的、复杂的环境下，如何保证用户的应用、数据清晰可控。简化认证管理、强化端到端的可信接入方面将会是云安全发展的方向之一。

3）Web 安全防护

云计算模式中，Web 应用是用户最直观的体验窗口，也是唯一的应用接口。而近几年风起云涌的各种 Web 攻击手段，则直接影响到云计算的顺利发展。

4）虚拟化安全

虚拟化是云计算的标志之一。然而，虚拟化的结果，却使许多传统的安全防护手段失效。从技术层面上讲，云计算与传统 IT 环境最大的区别在于其虚拟的计算环境，也正是这一区别导致其安全问题变得异常“棘手”。虚拟化的计算，使得应用进程间的相互影响更加难以捉摸；虚拟化的存储，使得数据的隔离与清除变得难以衡量；虚拟化的网络结构，使得传统的分域防护变得难以实现；虚拟化的服务提供模式，使得对使用者身份、权限和行为的鉴别、控制与审计变得极其重要。

5）云安全服务

面对云计算的安全问题，现如今有许多基于云服务提供的安全，包括 Web 和邮件过滤、网络流量访问控制和监控以及用于支付卡业务的标记化。不同安全服务的一个重要区别是，一些是“在云中”的而一些是“针对云”的，即那些集成到云环境中作为虚拟设备提供给用户使用和控制的安全服务。

在选择云安全服务时，要多同服务提供商沟通，了解他们能具体提供什么以及是否能满足自己的需求。为降低企业的风险，最好签订一份服务协议。

6.1.4　云计算安全关键技术

云计算安全关键技术主要包括虚拟机安全技术、海量用户的身份认证、隐私保护与数据安全等三个方面。

1. 虚拟机安全技术

虚拟机中的安全问题主要指针对虚拟机控制器的各类攻击（对虚拟机控制器的恶意修

改和嵌套等)，以及基于虚拟机的 Rootkit。目前针对这些问题，主要采用的防护方法有基于虚拟机的入侵检测，基于虚拟机的内核保护和基于虚拟机的可信计算等。

1）基于虚拟机的入侵检测技术

虚拟化技术带来了计算机系统结构的变化，也改变了传统安全软件的应用环境。目前，对虚拟机中的入侵检测技术的研究主要集中在基于主机的入侵检测上。但是，在实际的应用环境中，大部分的安全威胁都是来自于网络中，在虚拟机环境中对基于网络的入侵检测系统的研究更能有效地保障虚拟机的运行安全。

虚拟机利用虚拟机管理器来管理和调度多个客户操作系统对底层单一物理资源的共享访问。通过在虚拟机内部虚拟一个网桥设备，并把各个客户操作系统的网络设备挂接到该虚拟网桥上，由此虚拟机实现了对网络设备的虚拟化。由于虚拟机系统的出现导致传统的操作系统直接运行于硬件层之上的结构发生变化。在虚拟机系统之中，VMM 层位于硬件层和操作系统层之间，运行于系统最高特权级，由 VMM 实现对系统所有物理资源的虚拟化和调度管理；另外，同一个虚拟机平台上现在可以部署多台虚拟机，和传统的单一系统占据整台机器也有了本质的不同。这些特征都使得传统的入侵检测系统已经不能完全适应机器体系结构上发生的变化。

在一个虚拟机系统中，可以部署多个虚拟机，并且每个虚拟机部署不同的服务，因此会产生不同的安全级别，在面向虚拟机网络入侵检测系统的设计中，需要针对这些不同的安全级别采取不同的安全配置。同时，也能针对各个虚拟机进行单独配置，用户可以按照各个虚拟机所配置的服务类型选择所需要的服务。

在虚拟机中，由虚拟网桥负责转发虚拟机中所有的数据流，各个虚拟机的虚拟网络接口直接挂接在虚拟网桥的输出端，数据探测器部署在各个虚拟网络接口上，直接捕获到进出虚拟机的网络数据包，基于虚拟机的入侵检测机制如图 6-9 所示。

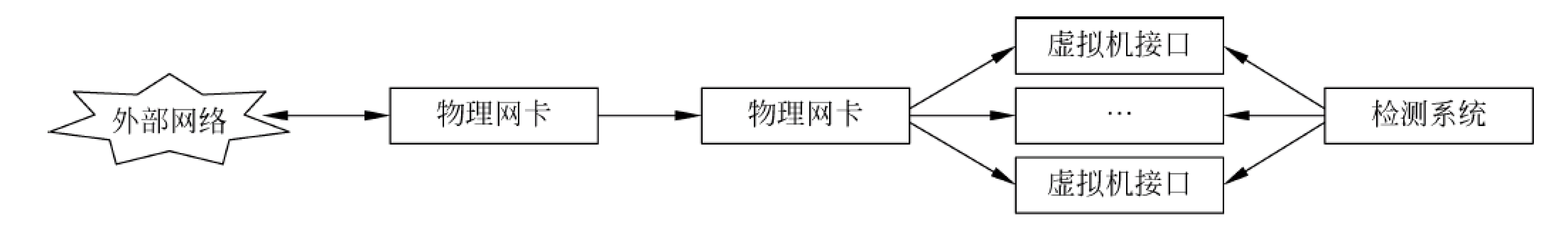


图 6-9 基于虚拟机的入侵检测机制

2）基于虚拟机的内核保护技术

基于虚拟机的 Rootkit 是运行在虚拟机系统内核空间的恶意程序，可以修改内核程序的控制流程，从而对虚拟环境的安全构成巨大威胁。而基于虚拟机的内核保护技术主要通过分析内核中影响程序控制流程的资源，并对这些资源进行保护，从而防止 Rootkit 对内核控制流程的篡改。

Rootkit 按其运行的权限不同可以分为应用层 Rootkit 和内核级 Rootkit。

(1) 应用层 Rootkit 主要是通过修改或替换系统工具或者系统库来达到其攻击目标，有的应用层 Rootkit 还会修改替换了的系统工具和系统库的最后修改时间，所以更具一定的欺骗性。目前对应用层 Rootkit 的主要检测方法是文件的完整性检查法，即新系统安装完毕后通过这类工具获得并保存系统的各种信息，比如校验和最后修改时间等等，检测的时候通过比较文件的当前信息和保存的基准信息，如果不匹配说明攻击发生。

(2) 内核层 Rootkit 主要攻击内核的系统调用表、中断描述符表等等。当内核被攻击后,其提供给应用层的信息将不可靠,因此很少有纯应用层工具能检测到内核级 Rootkit,即使能检测到某些内核级 Rootkit,但当此 Rootkit 升级后就失效了。

目前内核级检测工具通常都是应用层和内核层,或者是应用层和能结合/dev/[k]mem 设备文件比较可靠的获得内核某些信息的工具的结合。例如 kern_check、checkidt 和 StMichael 等。kern_check 主要手段是比较各个内核符号在 System.map 文件中的地址和系统运行时的地址;checkidt 主要通过检查中断描述符表的完整性,检测到攻击中断描述表这一特定类型 Rootkit;StMichael 主要手段是验证内核关键区域,如代码段和系统调用表的完整性来达到检测目的,它截获了可加载模块的加载等系统调用,在每次模块加载等操作时都会触发完整性的检查操作。它还设置了一个定时器,以固定时间间隔运行完整性检查操作。

3) 基于虚拟机的可信计算

虚拟机的可信计算也是虚拟机安全的一个重要发展方向。由斯坦福大学 Tal Garfinkel 等人提出的 Terra 结构是目前在虚拟机可信计算方面的代表,它提供了一个简单且可变通的设计模型,准许应用设计者在闭合平台上以同样的方法建立安全的应用。同时 Terra 支持目前的多数操作系统和应用。Terra 结构是通过可信虚拟机监控器(Trusted Virtual Machine Monitor,TVMM)来实现上面的目标的,TVMM 是一个高可信的虚拟机监控器,将单一的、抗攻击的通用平台划分成多个相互隔离的虚拟机。

通过可信虚拟监控器,现有的操作系统和应用都能运行在一个与现有开放平台类似的明箱(open-box)虚拟机上;它们也可以运行在一个提供专用闭合平台功能的自己的暗箱(closed-box)虚拟机之上。可信虚拟机监控器保护暗箱虚拟机内容的保密性和完整性,在暗箱虚拟机里运行的应用程序可以修改自己的软件堆以适应它们的安全要求。TVMM 还允许应用加密的向远端证明运行软件堆的身份,这一过程称之为证明(attestation)。

Terra 的核心是虚拟机监控器,像普通的虚拟机监控器一样,Terra 通过虚拟化硬件资源,使很多虚拟机能独立并发地运行,除此之外,它还提供额外的安全性能,如扮演信任方的角色向远端方证明虚拟机上软件的身份。

Terra 保障了虚拟机监控器是可信的。虚拟机监控器既是整个虚拟机安全的瓶颈,也是整个系统安全的基础,TVMM 保障了 VMM 的安全性,从而奠定了在 VMM 上实现其他软件的安全基础。面向虚拟机的网络入侵检测系统需要以安全的 VMM 为实现保障。

2. 海量用户的身份认证

在互联网时代的大型数据业务系统中,大量用户的身份认证和接入管理往往采用强制认证方式,例如指纹认证、USB Key 认证、动态密码认证等。但是在这种身份认证和管理主要是基于系统自身对于用户身份的不信任作为主要思想而设计的。在云计算时代,因为用户更加关心的云计算提供商是否按照 SLA 实施双方约定好的访问控制策略,所以在云计算模式下,研究者开始关注如何通过身份认证来保证用户自身资源或者信息数据等不会被提供商或者他人滥用。当前比较可行的解决方案就是引入第三方 CA 中心,由后者提供为双方所接受的私钥。

云计算系统应建立统一、集中的认证和授权系统,以满足云计算多租户环境下复杂的用

户权限策略管理和海量访问认证要求，提高云计算系统身份管理和认证的安全性。

1）集中用户认证

集中用户认证是指采用主流认证方式，如 LDAP、数字证书认证、令牌卡认证、硬件信息绑定认证、生物特征认证等，支持多因子认证。对不同类型和等级的系统、服务、端口采用相应等级的一种或多种组合认证方式，以满足云计算系统中不同子系统的安全等级与成本及易用性的平衡要求。提供用户访问日志记录，记录用户登录信息，包括系统标识、登录用户、登录时间、登录 IP、登录终端等标识。

2）集中用户授权

集中用户授权是指根据用户、用户组、用户级别的定义来对云计算系统资源的访问进行集中授权，采用集中授权或分级授权机制，支持细颗粒度授权策略。

3）访问授权策略管理身份认证策略

访问授权策略管理身份认证策略即采用用户身份与终端绑定的策略、完整性认证检查策略和口令策略。授权策略是指支持采用集中授权或分级授权策略。账号策略是指设置账号安全策略，包括口令连续错误锁定账号、长期不用导致账号失效、用户账号未退出时禁止重复登录等。

4）其他功能要求和日志管理

支持对用户认证信息、授权信息等详细日志的集中存储和查询。加密机制是指支持对认证、授权等敏感数据的加密存储及传输。

3. 隐私保护与数据安全技术

虽然云计算从服务提供方式上可以划分为 IaaS（基础设施即服务）、PaaS（平台即服务）和 SaaS（软件即服务）3 个层次，但本质上都是将数据中心外包给云计算服务提供商的模式。因此，如何保证用户数据的私密性及如何让用户相信他们的数据能够获得必要的隐私保护是云计算服务提供商需要特别关注的问题。用户隐私保护和数据安全主要包括各类信息的物理隔离或者虚拟化环境下的隔离；基于身份的物理或者虚拟安全边界访问控制；数据的异地容灾与备份以及数据恢复；数据的加密传输和加密存储；剩余信息保护等。在云计算应用中，数据量规模之巨已经远远超出传统大型 IDC 数据规模，同时不同用户对于隐私和数据安全的敏感度也各不相同。对数据隐私的保护是云计算服务能够被大众广泛认可并获得深入推广的必要前提，它要求为用户交付的服务的每一个环节都能得到安全性保证。

在数据传输方面，企业数据通过网络传递给云计算服务提供商进行处理，而这些数据中保存了大量企业的重要核心数据，如企业的销售数据、客户信息、财务信息等。如何确保企业的数据在网络传输过程中不被窃取、修改，保证数据的完整性、保密性和可利用性，需要对网络监测技术、数据加密技术和权限认证技术进行研究。在云计算应用环境下，数据传输加密可以选择在链路层、网络层、传输层甚至应用层等层面实现。主要的技术措施包括 IPSec VPN、SSL 等 VPN 技术，保证用户数据在网络传输中机密性、完整性和可用性。

在数据存储方面，企业数据存储在云中心，但用户并不清楚自己的数据被放置在哪一台服务器上，甚至根本不了解这台服务器放置在哪个地方，以及服务器所在地是否会有相关政策从而导致信息泄露。在这种数据存储资源的共享环境下，云计算服务提供商要能保证数据之间的有效隔离。另外，云计算服务提供商需要对企业托管的数据进行备份，以备在出现

重大事故时及时恢复用户数据,并且要保证数据本身及其所有备份在不需要时能被完全删除而不留任何痕迹。因此,云计算服务提供商必须针对这些问题对共享环境下的数据存储技术进行深入研发,以保证用户在任何时候都可以安全地访问数据。对于云存储类服务,一般的提供商都支持对数据进行加密存储,防止数据被他人非法窥探。一般会采用效能较高的对称加密算法,如 AES、3DES 等国际通用算法等。

在数据审计方面,在云计算模式下的企业审计需要借助云计算服务提供商的配合,并为第三方机构提供必要的信息支持,满足用户企业的数据审计需求。另外,云计算服务提供商的服务提供资质也很重要,要确保服务商在提供有效的云计算服务的同时不损害用户的利益。技术实力弱、难以长期存在的云计算服务提供商将带来很高的安全风险。

在运营策略方面,由于企业关键的数据存储在云端,用户会因为担心隐私被泄露而产生顾虑。云计算服务提供商需要对其运营策略进行改进,通过借助商业规则和信誉,树立良好的企业形象和公信力,在保障用户隐私的同时,又必须对用户行为进行必要的监督和管制。例如,云计算的按需提供资源并按需计费的模式降低了不良用户通过网络发起不良行为的成本,会助长其破坏互联网安全的行为。对于这类情况,云计算服务提供商必须给予监督并在政策指导下坚决予以打击,这也是服务提供商的安全责任所在。

6.1.5 云计算与物联网

1. 云计算与物联网关系

由于云计算从本质上来说就是一个用于海量数据处理的计算平台,因此,云计算技术是物联网涵盖的技术范畴之一。随着物联网的发展,未来物联网将势必产生海量数据,而传统的硬件架构服务器将很难满足数据管理和处理要求,如果将云计算运用到物联网的传输层和应用层,采用云计算的物联网,将会在很大程度上提高运作效率。

运用云计算模式,使物联网中数以兆计的各类物品的实时动态管理、智能分析变得可能。物联网通过将射频识别技术(RFID)、传感器技术、纳米技术等新技术充分运用在各行各业之中。将各种物体充分连接,并通过无线等网络将采集到的各种实时动态信息送达计算处理中心,进行汇总、分析和处理,从而将各种物体连接。

物联网和互联网的融合,需要更高层次的整合,需要“更透彻的感知、更全面的互联互通、更深入的智能化”。这同样也需要依靠高效的、动态的、可以大规模扩展的计算机资源处理能力,而这正是云计算模式所擅长的。同时,云计算的创新型服务交付模式,简化服务的交付,加强物联网和互联网之间及其内部的互联互通,可以实现新商业模式的快速创新,促进物联网和互联网的智能融合。

2. 云计算在物联网中的应用

将云计算的云计算、云储存、云服务、云终端等技术应用于物联网的感知层、应用层及网络层,从而解决物联网中海量信息和数据的管理问题。

1)节点不可信的问题

可以有效地解决服务器的节点不可信的问题,可以最大限度地降低服务器的出错概率。随着科技的不断进步发展,物联网已经从原来的局域网逐渐的发展成为城域网,其信息量也

随之不断增多，这样也就导致服务器的数量不断增加，从而导致节点的出错概率的增加。在云计算中，可以有不同数目的虚拟服务器组，其可以按照先来先提供服务的方式，以此来完成节点之间的分布式的调度，这样在屏蔽相关节点的时候，也会提升相应的速率，云计算可以有效地保障物联网无间断安全服务的实现。

2）获得很好的经济收益

可以保障物联网在低的投入下，获得很好的经济收益。一般情况下，服务器的硬件资源都是有一定限度的，当服务器的响应数量超出了自身承载数量的最大值，可能会造成服务器的瘫痪现象的发生。而云计算的出现，就可以通过采用机群均衡的调度方式，在服务器访问数量达到最大的负载的时候，通过改变服务的等级，以此来动态的减少或者是增加服务器的数量以及质量，达到释放访问压力的效果。

3）实现物联网的广泛连接

可以实现物联网由局域网到互联网的广泛连接，能够很大程度上对信息资源进行共享，能够保障物联网的相关信息放在互联网的云计算中心上，这样就能够保障信息的空间性。在任何地方只要有相应的传感器芯片，就能够从服务器中收到相关的信息。

3. 云计算与物联网中的结合方式

云计算与物联网的结合方式我们可以分为以下几种。

1）单中心，多终端

在此类模式中，分布范围较小的各个物联网终端（传感器、摄像头或 3G 手机等），把云中心或部分云中心作为数据/处理中心，终端所获得信息、数据统一由云中心处理及存储，云中心提供统一界面给使用者操作或者查看。

这类应用非常多，如小区及家庭的监控、对某一高速路段的监测、幼儿园小朋友监管以及某些公共设施的保护等。实现这类应用的云中心，可提供海量存储和统一界面、分级管理等功能，对日常生活提供较好的帮助。一般此类云中心以私有云居多。

2）多中心，大量终端

对于很多区域跨度较大的企业、单位而言，多中心、大量终端的模式较适合。譬如，一个跨多地区或者多国家的企业，因其分公司或分厂较多，要对其各公司或工厂的生产流程进行监控、对相关的产品进行质量跟踪等等。

同理，当有些数据或者信息需要及时甚至实时共享给各个终端的使用者时，也可采取这种方式。举个简单的例子，假如北京地震中心能预测到某地 10 分钟后会有地震，只需要通过这种途径，仅仅十几秒就能将地震的危急警告信息发出，可尽量避免不必要的损失。中国联通的“互联云”思想就是基于此思路提出的。这个的模式的前提是我们的云中心必须包含公共云和私有云，并且他们之间的互联没有障碍。这样，对于有些机密的事情，比如企业机密等可较好地保密而又不影响信息的传递与传播。

3）信息与应用分层处理、海量终端

这种模式可以针对用户的范围广、信息及数据种类多、安全性要求高等特征来打造。当前，客户对各种海量数据的处理需求越来越多，针对此情况，我们可以根据客户需求及云中心的分布进行合理的分配。对需要大量数据传送，但是安全性要求不高的，如视频数据、游戏数据等，我们可以采取本地云中心处理或存储。对于计算要求高，数据量不大的，可以放

在专门负责高端运算的云中心里。而对于数据安全要求非常高的信息和数据,我们可以放在具有灾备中心的云中心里。

4. 云计算与物联网结合面临的问题

1）规模问题

规模化是云计算与物联网结合的前提条件。只有当物联网的规模足够大之后,才有可能和云计算结合起来,比如行业应用中的智能电网、地震台网监测等等需要云计算。而对一般性的、局域的、家庭网的物联网应用,则没有必要结合云计算。如何使两者发展至相应规模,尚待解决。

2）安全问题

无论是云计算还是物联网,都有海量的物、人相关的数据。若安全措施不到位,或者数据管理存在漏洞,它们将使我们的生活无所遁形。使我们面临黑客、病毒的威胁,甚或被恐怖分子轻易跟踪、定位,这势必带来对个人隐私的侵犯和企业机密泄露等问题。破坏了信息的合法有序使用要求,可能导致人们的生活、工作陷入瘫痪,社会秩序混乱。因此,这就要求政府、企业、科研院所等各有关部门运用技术、法律、行政等各种手段,解决安全问题。

3）网络连接问题

云计算和物联网都需要持续、稳定的网络连接,以传输大量数据。如果在低效率网络连接的环境下,则不能很好工作,难以发挥应用的作用。因此,如何解决不同网络(有线网络、无线网络)之间的有效通信,建立持续、大容量、高可靠的网络连接,需要深入研究。

4）标准化问题

标准是对任何技术的统一规范,由于云计算和物联网都是由多设备、多网络、多应用通过互相融合形成的复杂网络,需要把各系统都通过统一的接口、通信协议等标准联系在一起。这将是在两者中不断发展,有效健全的问题。

总之,物联网是指“把所有物品通过射频识别等信息传感设备与互联网连接起来,实现智能化识别和管理”;云计算是指“利用互联网的分布性等特点来进行计算和存储”。前者是对互联网的极大拓展,而后者则是一种网络应用模式,两者存在着较大的区别。

然而,对于物联网来说,本身需要进行大量而快速的运算,云计算带来的高效率的运算模式正好可以为其提供良好的应用基础。没有云计算的发展,物联网也就不能顺利实现,而物联网的发展又推动了云计算技术的进步,因为只有真正与物联网结合后,云计算才算是真正意义上从概念走向应用,两者缺一不可。

6.2 中间件安全

6.2.1 中间件概述

顾名思义,中间件(Middleware)是处于操作系统与应用程序中间的软件。中间件的结构如图6-10所示。

在众多关于中间件的定义中,被各界广泛接受的是IDC的表述,即中间件是一种独立的系统软件或服务程序,分布式应用软件借助这种软件在不同的技术之间共享资源,中间件

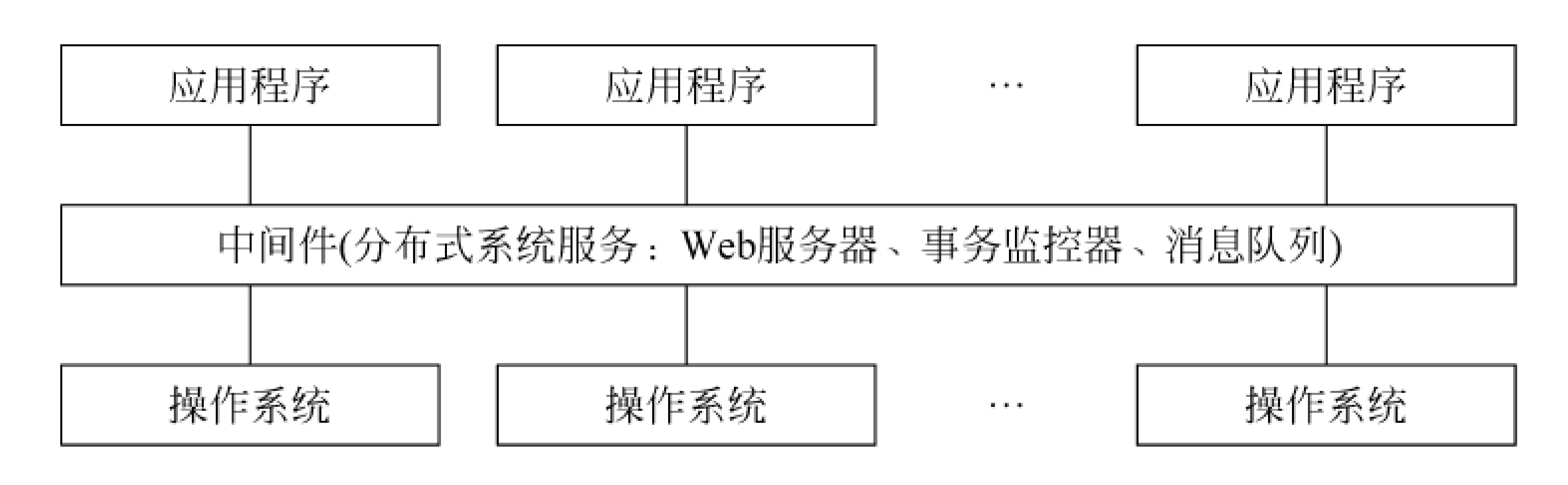


图 6-10 中间件的结构

位于客户机服务器的操作系统之上，管理计算资源和网络通信。

IDC 对中间件的定义表明，中间件是一类软件，而非一种软件；中间件不仅仅实现互连，还要实现应用之间的互操作；中间件是基于分布式处理的软件，最突出的特点是其网络通信功能。

中间件是基础软件的一大类，属于可复用软件的范畴。人们在使用中间件时，往往将一组中间件集成在一起，构成一个平台(包括开发平台和运行平台)，但在这组中间件中必需要有一个通信中间件，即中间件＝平台＋通信。这个定义也限定了只有用于分布式系统中才能称为中间件，同时还可以把它与操作系统和应用软件区分开来。

中间件是一类连接软件组件和应用的计算机软件。它包括一组服务，以便于运行在一台或多台计算机上的多个软件通过网络进行交互。该技术所提供的互操作性，推动了一致分布式体系架构的演进。中间件架构通常用于支持分布式应用软件，并简化了其复杂程度。它包括 Web 服务器、事务监控器和消息队列软件等。

目前，中间件技术发展很快，已经与操作系统和数据库并列为 3 大基础软件。

中间件位于操作系统、网络和数据库的上层，应用程序的下层。中间件的核心作用是通过管理计算资源和网络通信，为各类分布式应用软件共享资源提供支撑。广义地看，中间件的总体作用是为处于自己上层的应用软件提供运行与开发的环境，帮助用户灵活地、高效地开发和集成复杂的应用软件。

中间件的产生与迅速发展的原因如表 6-1 所示。

表 6-1 操作系统、数据库管理系统与中间件的比较

基础软件类型	操作系统	数据库管理系统	中间件
产生原因	硬件过于复杂	数据过于复杂	网络环境过于复杂
主要作用	管理各种资源	管理各类数据	支持不同的交互模式
理论基础	各种调度算法	各种数据模型	各种协议、各种接口
产品形态	功能类似	功能类似	种类多，功能差别大

由于计算机网络环境的日益复杂，为了支持各种不同的交互模式，产生了适应各种不同网络环境和应用系统的中间件。

6.2.2 中间件的分类

中间件所包括的范围十分广泛，针对不同的应用需求涌现出多种各具特色的中间件产品。但至今中间件还没有一个比较精确的定义，因此，在不同的角度或不同的层次上，对中

间件的分类也会有所不同。由于中间件需要屏蔽分布环境中异构的操作系统和网络协议,它必须能够提供分布环境下的通信服务,我们将这种通信服务称之为中间件平台。

基于目的和实现机制的不同,可以将中间件平台分为以下几类:远程过程调用(Remote Procedure Call Middleware, RPC)、面向消息的中间件(Message-Oriented Middleware,MOM)、对象请求代理(Object Request Broker,ORB)和事务处理监控(Transaction Processing Monitor,TPM)。

它们可向上提供不同形式的通信服务,包括同步、排队、订阅发布、广播等等,在这些基本的通信平台之上,可构筑各种框架,为应用程序提供不同领域内的服务,如事务处理监控器、分布数据访问、对象事务管理器 OTM 等。平台为上层应用屏蔽了异构平台的差异,而其上的框架又定义了相应领域内的应用系统结构、标准的服务组件等,用户只须告诉框架所关心的事件,然后提供处理这些事件的代码。当事件发生时,框架则会调用用户的代码。用户代码不用调用框架,用户程序也不必关心框架结构、执行流程、对系统级 API 的调用等,所有这些由框架负责完成。因此,基于中间件开发的应用具有良好的可扩充性、易管理性、高可用性和可移植性。

1. 远程过程调用

远程过程调用(Remote Procedure Call,RPC)是一种广泛使用的分布式应用程序处理方法。一个应用程序使用 RPC 来“远程”执行一个位于不同地址空间里的过程,并且从效果上看和执行本地调用相同。事实上,一个 RPC 应用分为两个部分: Server 和 Client。Server 提供一个或多个远程过程; Client 向 Server 发出远程调用。Server 和 Client 可以位于同一台计算机,也可以位于不同的计算机,甚至运行在不同的操作系统之上。它们通过网络进行通信。Client 运行相应的 Server 提供的数据转换和通信服务,从而屏蔽不同的操作系统和网络协议。在这里 RPC 通信是同步的,采用线程可以进行异步调用。

在 RPC 模型中,Client 和 Server 只要具备了相应的 RPC 接口,并且具有 RPC 运行支持,就可以完成相应的互操作,而不必限制于特定的 Server。因此,RPC 为 Client/Server 分布式计算提供了有力地支持。同时,远程过程调用 RPC 所提供的是基于过程的服务访问,Client 与 Server 进行直接连接,没有中间机构来处理请求,因此也具有一定的局限性。比如,RPC 通常需要一些网络细节以定位 Server; 在 Client 发出请求的同时,要求 Server 必须是活动的等等。

2. 面向消息的中间件

面向消息的中间件(Message-Oriented Middleware, MOM)指的是利用高效可靠的消息传递机制进行平台无关的数据交流,并基于数据通信来进行分布式系统的集成。通过提供消息传递和消息排队模型,它可在分布环境下扩展进程间的通信,并支持多通信协议、语言、应用程序、硬件和软件平台。流行的 MOM 中间件产品有 IBM 的 MQSeries、BEA 的 MessageQ 等。消息传递和排队技术有以下三个主要特点:

1) 通信程序可在不同的时间运行

程序不在网络上直接相互通话,而是间接地将消息放入消息队列,因为程序间没有直接的联系。所以它们不必同时运行。消息放入适当的队列时,目标程序甚至根本不需要正在

运行；即使目标程序在运行，也不意味着要立即处理该消息。

2）对应用程序的结构没有约束

在复杂的应用场合中，通信程序之间不仅可以是一对一的关系，还可以进行一对多和多对一方式，甚至是上述多种方式的组合。多种通信方式的构造并没有增加应用程序的复杂性。

3）程序与网络复杂性相隔离

程序将消息放入消息队列或从消息队列中取出消息来进行通信，与此关联的全部活动，比如维护消息队列、维护程序和队列之间的关系、处理网络的重新启动和在网络中移动消息等是 MOM 的任务，程序不直接与其他程序通话，并且它们不涉及网络通信的复杂性。

3. 对象请求代理中间件

随着对象技术与分布式计算技术的发展，两者相互结合形成了分布对象计算，并发展为当今软件技术的主流方向。1990 年底，对象管理集团 OMG 首次推出对象管理结构（Object Management Architecture，OMA），对象请求代理中间件（Object Request Broker，ORB）是这个模型的核心组件。它的作用在于提供一个通信框架，透明地在异构的分布计算环境中传递对象请求。CORBA 规范包括了 ORB 的所有标准接口。1991 年推出的 CORBA 1.1 定义了接口描述语言 OMG IDL 和支持 Client/Server 对象在具体的 ORB 上进行互操作的 API。CORBA 2.0 规范描述的是不同厂商提供的 ORB 之间的互操作。

对象请求代理是对象总线，它在 CORBA 规范中处于核心地位，定义异构环境下对象透明地发送请求和接收响应的基本机制，是建立对象之间 client/server 关系的中间件。ORB 使得对象可以透明地向其他对象发出请求或接受其他对象的响应，这些对象可以位于本地也可以位于远程机器。ORB 拦截请求调用，并负责找到可以实现请求的对象、传送参数、调用相应的方法、返回结果等。Client 对象并不知道同 Server 对象通信、激活或存储 Server 对象的机制，也不必知道 Server 对象位于何处、它是用何种语言实现的、使用什么操作系统或其他不属于对象接口的系统成分。

值得指出的是 Client 和 Server 角色只是用来协调对象之间的相互作用，根据相应的场合，ORB 上的对象可以是 Client，也可以是 Server，甚至两者兼有。当对象发出一个请求时，它是处于 Client 角色；当它在接收请求时，它就处于 Server 角色。大部分的对象都是既扮演 Client 角色又扮演 Server 角色。另外由于 ORB 负责对象请求的传送和 Server 的管理，Client 和 Server 之间并不直接连接，因此，与 RPC 所支持的单纯的 Client/Server 结构相比，ORB 可以支持更加复杂的结构。

4. 事务处理监控中间件

事务处理监控（Transaction Processing Monitor，TPM）最早出现在大型机上，为其提供支持大规模事务处理的可靠运行环境。随着分布计算技术的发展，分布应用系统对大规模的事务处理提出了需求，比如商业活动中大量的关键事务处理。事务处理监控界于 Client 和 Server 之间，进行事务管理与协调、负载平衡、失败恢复等，以提高系统的整体性能。它可以被看作是事务处理应用程序的“操作系统”。总体上来说，事务处理监控有以下功能。

1）进程管理

进程管理包括启动 Server 进程、为其分配任务、监控其执行并对负载进行平衡。

2）事务管理

事务管理即保证在其监控下的事务处理的原则性、一致性、独立性和持久性。

3）通信管理

通信管理为 Client 和 Server 之间提供了多种通信机制，包括请求响应、会话、排队、订阅发布和广播等。

事务处理监控能够为大量的 Client 提供服务，比如飞机订票系统。如果 Server 为每一个 Client 都分配其所需要的资源的话，那 Server 将不堪重负。但实际上，在同一时刻并不是所有的 Client 都需要请求服务，而一旦某个 Client 请求了服务，它希望得到快速的响应。事务处理监控在操作系统之上提供一组服务，对 Client 请求进行管理并为其分配相应的服务进程，使 Server 在有限的系统资源下能够高效地为大规模的客户提供服务。

6.2.3　RFID 中间件

1. RFID 中间件的工作原理

RFID 中间件扮演 RFID 的标签和应用程序之间的中介角色，从应用程序端使用中间件提供一组通用的应用程序接口（API）。中间件可以连接到 RFID 的读写器，读取 RFID 标签中的数据。因此，尽管存储 RFID 标签信息的数据库软件或后端应用程序被修改或被其他软件取代，甚至 RFID 读写器的种类发生变化等情况发生时，应用端不须修改也同样能够处理。这样，解决了多对多连接的维护复杂性问题。

RFID 中间件是一种面向消息的中间件，信息以消息的形式从一个程序传送到另一个或多个程序。信息可以以异步的形式传送，所以传送者不必等待响应。面向消息的中间件包含的功能不仅是传递信息，还必须包括解译数据、安全性、数据广播、错误恢复、定位网络资源、找出成本最低的路径、消息与要求的优先次序以及延伸的除错工具等服务。

2. RFID 中间件的分类

RFID 中间件可以从架构上分为两类。

1）以应用程序为中心

这种设计模式是通过 RFID 读写器厂商提供的应用程序接口，以 Hot Code 方式直接编写特定的 RFID 阅读器的读写数据适配器，并传送至后端系统的应用程序或数据库，从而达到与后端系统或服务连接的目的。

2）以软件架构为中心

随着企业物联网应用系统复杂度的提高，企业将无法负荷以 Hot Code 方式为每个应用程序编写适配器，同时还将会面临对象标准化等技术难题。此时，企业可以考虑采用厂商提供的标准规格的 RFID 中间件。这样，尽管发生 RFID 标签信息的数据库软件改由其他软件替代，或者 RFID 标签的读写器种类变化等情况，应用端也不需要做任何修改。

3. RFID 中间件的特点

1）独立与架构

RFID 中间件独立并介于 RFID 的读写器与后端应用程序之间，并且能够与多个 RFID

读写器以及多个后端应用程序连接，从而减轻架构和维护的复杂性。

2）数据流

RFID 的主要目的是将实体对象转换为信息环境下的虚拟对象，因此数据处理是 RFID 的最重要的功能。RFID 中间件具有数据的收集、过滤、整合与传递等特性，以便将正确的对象信息传送到企业后端的应用系统。

3）处理流

RFID 中间件采用程序逻辑以及存储再转送的功能来提供顺序的消息流，具有数据流的设计与管理的能力。

4）标准

RFID 系统为自动数据采样技术与辨析实体对象的应用。EPC global 制定了适用于全球各种产品的唯一识别号码的统一标准，即电子产品编码（Electronic Product Code，EPC）。EPC 在供应链系统中以一串数字来识别某种特定的商品。通过无线射频辨识标签，由 RFID 的读写器读入后，传送到计算机或应用系统中的过程称为对象命名服务。对象命名服务系统会锁定计算机网络中的固定点，抓取有关商品的信息。EPC 存放在 RFID 的标签中，被 RFID 读写器读出后，即可提供追踪 EPC 所对应的物品名称及相关信息，并立刻识别和分享供应链中的物品数据，显著地提高了信息的透明度。

4. RFID 中间件的发展

从发展趋势来分析，RFID 中间件可以分为以下三个发展阶段：

1）中间件应用程序阶段

RFID 初期的发展，多以整合串接 RFID 读写器为目的。在这个阶段，RFID 生产厂商一般都主动提供简单的应用程序接口（API），供企业将后端系统与 RFID 读写器连接。从整体发展架构来看，此时企业的导入必须自行花费许多成本去处理前后端系统的连接问题。通常，企业在这个阶段会通过试点工程方式来评估成本效益与导入的关键问题。

2）中间件架构阶段

中间件架构阶段是 RFID 中间件成长的关键阶段。由于 RFID 的强大应用，沃尔玛与美国国防部等关键使用机构相继进行 RFID 技术的规划，并进行导入的试点工程，促使大型厂商持续关注 RFID 相关市场的发展。在这个阶段，随着 RFID 中间件的发展，它不但已经具备基本数据收集、过滤等功能，同时也满足了企业多对多的连接需求，并且具备平台的管理和维护功能。

3）中间件解决方案阶段

在 RFID 标签、读写器与中间件的发展成熟过程中，各大厂商针对不同领域提出了各项创新应用解决方案。例如，曼哈特联合软件公司提出了 RFID 一盒子解决方案（RFID in a box），企业不需要再为前端 RFID 的硬件与后端应用系统的连接而烦恼。曼哈特联合软件公司与艾邻技术公司在 RFID 硬件端合作，开发了以 Microsoft. Net 平台为基础的中间件。原本使用曼哈特联合软件公司供应链执行解决方案的 900 多家企业，只需要通过 RFID 一盒子解决方案，就可以在原有应用系统上快速利用 RFID 来加强供应链管理的透明度。

5. RFID 中间件技术的发展现状

1）国际 RFID 中间件产品的发展现状

最早提出 RFID 中间件概念的国家是美国。美国企业在实施 RFID 项目改造期间，发现最耗时、耗力、复杂度和难度最高的问题，是如何保证 RFID 数据正确导入企业的管理系统。为此企业做了大量的工作用于保证 RFID 数据的正确性。经过企业与研究机构的多方研究、论证、实验，终于找到了一个比较好的解决方法，这就是 RFID 中间件。

目前，在国际上比较知名的 RFID 中间件厂商，有 IBM、Oracle、Microsoft、SAP、Sun、Sybase、BEA 等国际知名企业。由于这些软件厂商本身就具备比较雄厚的技术实力，其开发的 RFID 中间件产品又经过实验室、企业实地的反复测试，因此，这些 RFID 中间件产品的稳定性、先进性、海量数据的处理能力都比较完善，得到了企业的广泛认可。

（1）IBM RFID 中间件。

IBM RFID 中间件是一套基于 Java 并遵循 J2EE 企业架构开发的一套开放式 RFID 中间件产品，可以帮助企业简化实施 RFID 项目的步骤，能满足企业处理海量货物数据的要求；基于高度标准化的开发方式，IBM 的 RFID 中间件产品可以与企业信息管理系统无缝连接，有效缩短企业的项目实施周期，降低了 RFID 项目实施出错率，降低了企业的实施成本。

目前 IBM RFID 中间件产品已经成功应用于全球第四大零售商 Metro 公司的供应链之中，不仅提高了整个供应链商品的流转速度、减少了产品差错率，还提高了整个供应链的服务水平，降低了整个供应链的运营成本。此外，还有约 80 多家供应商表示，将与 IBM 公司签订采用这项新的 IBM WebSphere RFID 中间件解决方案。

为了进一步提高 RFID 解决方案的竞争力，目前 IBM 与 Intermec 公司进行合作，将 IBM RFID 中间件成功地嵌入 Intermec 的 IF5 RFID 读写器中，共同向企业提供一整套 RFID 企业或供应链解决方案。

（2）Oracle RFID 中间件。

Oracle RFID 中间件是甲骨文公司着眼于未来 RFID 的巨大市场而开发的一套基于 JAVA 遵循 J2EE 企业架构的中间件产品。Oracle 中间件依托 Oracle 数据库，充分发挥 Oracle 数据库的数据处理优势，满足企业对海量 RFID 数据存储和分析处理的要求。Oracle RFID 中间件除最基本的数据功能外，还向用户提供了智能化的手工配置界面。实施 RFID 项目的企业可根据业务的实际需求，手工设定 RFID 读写器的数据扫描周期、相同数据的过滤周期，并指定 RFID 中间件将电子数据导入指定的服务数据库，并且企业还可以利用 Oracle 提供的各种数据库工具对 RFID 中间件导入的货物数据进行各种指标数据分析，并做出准确的预测。

（3）Microsoft 的 RFID 中间件。

微软公司在 RFID 巨大的市场面前自然不会袖手旁观，投入巨资组建了 RFID 实验室，着手进行 RFID 中间件和 RFID 平台的开发，并以微软 SQL 数据库和 Windows 操作系统为依托，向的大、中、小型企业提供 RFID 中间件企业解决方案。

与其他软件厂商运行的 JAVA 平台不同，Microsoft 中间件产品主要运行于微软的 Windows 系列操作平台。企业在选用中间件技术时，一定要考虑 RFID 中间件产品与自己

现有的企业管理软件的运行平台是否兼容。

根据微软的 RFID 中间件计划，微软准备将 RFID 中间件产品集成为 Windows 平台的一部分，并专门为 RFID 中间件产品的数据传输进行系统级的网络优化。依据 Windows 占据的全球市场份额及 Windows 平台优势，微软的 RFID 中间件产品拥有了更大的竞争优势。

(4) SAP 中间件。

SAP RFID 中间件产品也是基于 Java 语言遵循 J2EE 企业架构开发的产品。SAP RFID 中间件产品具有两个显著的特征：系列化产品和整合中间件。首先，SAP 的 RFID 中间件产品是系列化产品；其次，SAP 的 RFID 中间件是一个整合中间件，它可以将其他厂商的 RFID 中间件产品整合在一起，作为 SAP 整个企业信息管理系统应用体系的一部分进行实施。

SAP RFID 的中间件产品主要包括：SAP 自动身份识别基础设施软件、SAP 事件管理软件和 SAP 企业门户。为增强 SAP RFID 中间件的企业竞争力，SAP 又联合 Sun 和 Sybase，将这两家的 RFID 中间件产品整合到 SAP 的中间件产品中。与 Sybase 的 RFID 安全中间件整合，大大提高了 SAP 中间件数据传输的安全性；与 Sun 的 RFID 中间件结合，则使得 SAP 中间件的功能得到了极大的扩展。

SAP 的企业用户大多数是世界 500 强企业，原来已经采用 SAP 的管理系统。这些企业实施 RFID 项目的规模一般都比较大，对相关软件和硬件的性能要求也比较高。这些企业实施 RFID 项目改造，应用 SAP 提供的 RFID 中间件技术可以和 SAP 的管理系统实现无缝集成，能为企业节省大量的软件测试时间、软件的集成时间，有效缩短了 RFID 项目实施步骤和时间。

(5) Sun 的 RFID 中间件。

Sun 公司开发的 JAVA 语言，目前被广泛应用于开发各种企业级的管理软件。目前，Sun 公司根据市场需求，利用 JAVA 在企业的应用优势开发的 RFID 中间件，也具有独特的技术优势。

Sun 公司开发的 RFID 中间件产品从 1.0 版本开始，经历了较长时间的测试，随着产品不断完善，已经完全达到了设计要求。随着 RFID 标准 Gen 2.0 的推出，目前 Sun 中间件已推出了 2.0 版本，实现了 RFID 中间件对 Gen 2.0 版本的全面支持和中央系统管理。

其中间件分为事件管理器和信息服务器两个部分。事件管理器用来帮助处理通过 RFID 系统收集的信息或依照客户的需求筛选信息；信息服务器用来得到和存储使用 RFID 技术生成的信息，并将这些信息提供给供应链管理系统中的软件系统。

由于 Sun 公司在 RFID 中间件系统中集成了 Jini 网络工具，有新的 RFID 设备接入网络时，立刻能被系统自动发现并集成到网络中，实现新设备数据的自动收集。这一功能在储存库环境中是非常实用的。

为了进一步扩大 Sun RFID 中间件产品的影响力，Sun 公司已经与 SAP 等几家厂商组建了 RFID 中间件联盟，将各个厂家的 RFID 中间件产品整合到一起，利用各自的企业资源，进行 RFID 中间件产品推广工作。

(6) Sybase 中间件。

Sybase 原来是一家数据库公司，其开发的 Sybase 数据库在 20 世纪 80～90 年代曾辉煌

一时。在收购 Xcellenet 公司后，Sybase 公司正式介入 RFID 中间件领域，并开始使用 Xcellenet 公司技术开发 RFID 中间件产品。

Sybase 中间件包括 Edgeware 软件套件、RFID 业务流程、集成和监控工具。该工具采用基于网络的程序界面，将 RFID 数据所需要的业务流程映射到现有企业的系统中。客户可以建立独有的规则，并根据这些规则监控实时事件流和 RFID 中间件取得的信息数据。

Sybase 中间件的安全套件被 SAP 看中，被 SAP 整合进 SAP 企业应用系统，双方还签订了 RFID 中间件联盟协议，利用双方资源共同推广 RFID 中间件的企业 RFID 解决方案。

（7）BEA 的 RFID 中间件。

BEA RFID 中间件是目前 RFID 中间件领域最具竞争力的产品之一。尤其是在 2005 年 BEA 收购了 RFID 中间件技术领域的领先厂商 ConnecTerra 公司之后，ConnecTerra 的中间件整合进 BEA 的中间件产品，使 BEA 的 RFID 中间件功能得到极大的扩展。BEA 可以向企业提供完整的一揽子产品解决方案，帮助企业方便地实施 RFID 项目，帮助客户处理从供应链上获取的日益庞大的 RFID 数据。

BEA 公司的 RFID 解决方案由以下四个部分构成。

① BEA WebLogic RFID Edition：先进的 EPC 中间件，支持多达 12 个读写器提供商的主流读写器，支持 EPC Class0、0＋、1，ISO15693，ISO18000-6Bv1.19EPC，GEN2 等规格的电子标签；

② BEA WebLogic Enterprise Platform：专门为构建面向服务型企业解决方案而设计的统一的、可扩展的应用基础架构；

③ BEA RFID 解决方案工具箱：是实施 RFID 解决方案的加速器，包含快速配置和部署 RFID 应用系统所必需的代码、文档和最佳实践路线。主要内容包括事件模型框架、消息总线架构、预置的 portlet 等；

④ 为开发、配置和部署该解决方案提供帮助的咨询服务。该解决方案可以为客户实施 RFID 应用提供完整的基础架构，用户可以围绕 RFID 进行业务流程创新，开发新的应用，从而提高 RFID 项目投资的回报率。

目前，BEA 已成为基于标准的端到端 RFID 基础设施——从获取原始的 RFID 事件，直到把这些事件转换成重要的商业数据的厂家。

2）中国 RFID 中间件的发展现状

RFID 技术进入中国的时间比较短，各方面的工作还处于起步阶段。虽然中国政府在国家十一五规划和 863 计划中，对 RFID 应用提供了政策、项目和资金的支持，并且 RFID 在国内的发展也较为迅速，但是与国际先进技术的发展相比，在很多方面还存在明显的差距。

中国在 RFID 中间件和公共服务方面已经开展了一些工作。依托国家 863 计划“无线射频关键技术研究与开发”课题，中科院自动化所开发了 RFID 公共服务体系基础架构软件和血液、食品、药品可追溯管理中间件；华中科技大学开发了支持多通信平台的 RFID 中间件产品 Smarti；上海交通大学开发了面向商业物流的数据管理与集成中间件平台。此外，国内产品还包括东方励格公司的 LYNKO-ALE 中间件、清华同方的 ezRFID 中间件、ezONE、ezFramework 基础应用套件等。

目前，虽然中国已经有了一些初具规模的 RFID 中间件产品，但大多数都还没有在企业

进行实际应用测试，与国外的RFID中间件产品相比，尚处于实验室阶段。相对于国外经历了很长时间企业实际测试的成熟的RFID中间件产品，我国的RFID产品还有较大的差距。国内的相关企业和研发机构应尽快完成RFID中间件产品的企业测试，完善RFID中间件的相关功能，为国内中小企业的RFID项目实施提供方便、实用、低成本的RFID中间件解决方案。

如果中国的研发机构能够赶在企业开始大规模实施RFID项目之前，开发出完善、成熟、可靠的RFID中间件产品，加上天时、地利、人和、成本等优势，占据中国国内的RFID中间件市场是完全有可能的。

通过对比国内外RFID中间件的实际情况，不难发现，国外的RFID中间件产品发展的时间并不比中国RFID中间件早很多；只要中国的RFID研发机构与生产厂商奋起直追，依托国内较低的成本优势、众多优秀的软件工程师和技术人员共同努力，在短时间内完全有可能开发出与国外的同类产品相匹敌的RFID中间件产品。

6.2.4 RFID中间件安全

物联网是一个在互联网的基础上，结合RFID技术和传感器技术构建的连接范围更为广阔的网络。因此，物联网安全既包括当前互联网的安全问题，又包括RFID和传感器技术特有的安全问题。由于物联网感知识别层中大量应用RFID标签和无线传感器，因此物联网特有的安全问题，主要是RFID系统安全和无线传感器网络安全。RFID标签中保存着个人私密信息，随着定位技术的发展，假如RFID标签受到跟踪、定位，或者个人私密信息受到窃取，就会对用户的隐私造成伤害。

1. 中间件安全设计原则

RFID中间件的设计，要遵循功能全面、容易设计、便于维护、具有良好的扩展性和可移植性的原则。设计RFID中间件至少要解决以下几个问题。

(1) 屏蔽下层硬件，兼容不同的RFID读写器。

不同生产厂家的硬件设备在读取频率、支持协议、读写范围、防冲突性能等方面有所差异。因此屏蔽物理设备的差异，能方便地进行集成扩展，这是RFID中间件应具有的特点。

(2) 对硬件设备进行统一管理。

对硬件设备进行统一管理，包括打开、关闭、获取设备参数、发出读取指令、缓存标签、定义逻辑阅读器等，使上层的软件感觉不到设备的差异，提供透明的硬件服务。

(3) 对数据流进行过滤和分组。

安全中间件必须采用特定的算法和数据结构，过滤和剔除用户不感兴趣的、大量的、重复的、无规则的数据，否则，大量的垃圾数据流入上层，对企业应用程序将是一个沉重的负担，甚至会造成上层应用程序崩溃。

(4) 数据接收和数据格式转换。

中间件要接收来自RFID设备的标签数据，并向上层传输。由于数据标签编码方式多种多样，规范标准不统一，如果不进行数据格式处理，将会导致数据混乱，难以识别。

(5) 中间件的安全问题。

电子标签的安全和隐私问题，制约着EPC技术的发展和应用。RFID系统在进行数据

采集和数据传输时，电子标签和读写器容易受到信号的干扰，再加上电子标签容易被跟踪和定位，侵犯个人隐私，因此安全问题不可避免。

（6）与企业应用程序的通信。

企业应用程序具有自己特定的数据格式，采用何种方式与中间件进行交互，并且高效地实现中间件与应用程序之间的数据交换，也是中间件需要解决的重要问题。

2. 通用的中间件安全模型

针对中间件的安全需求，中国学者吴景阳和毋国庆等提出了一种通用的中间件安全模式。由于针对中间件层的特点进行分析，他们认为访问控制的实现依赖于引用监视器和访问策略的所在位置和实施。因此，可以根据安全逻辑的实现，将引用监视器的功能分成决策和执行两部分。

1）决策部分

决策部分根据访问策略来决定一个主体是否具有权限来访问它所请求的客体资源，采用决策机制可以是自主访问控制，也可以是强制访问控制，或者是其他机制。

2）执行部分

执行部分接受主体的访问请求，该请求是通过下层传送上来的，由执行部分负责将该请求传递给中间层中的决策部分，并将执行结果返回决策部分。执行部分根据此决策来执行相应的动作，如果访问被允许，则根据访问请求将主体的请求信息传送给目标对象。如果需要的话，可能还要调用中间件的其他部件，执行某些特定的功能，如事务处理、数据库访问等。

通用中间件安全模式如图 6-11 所示。

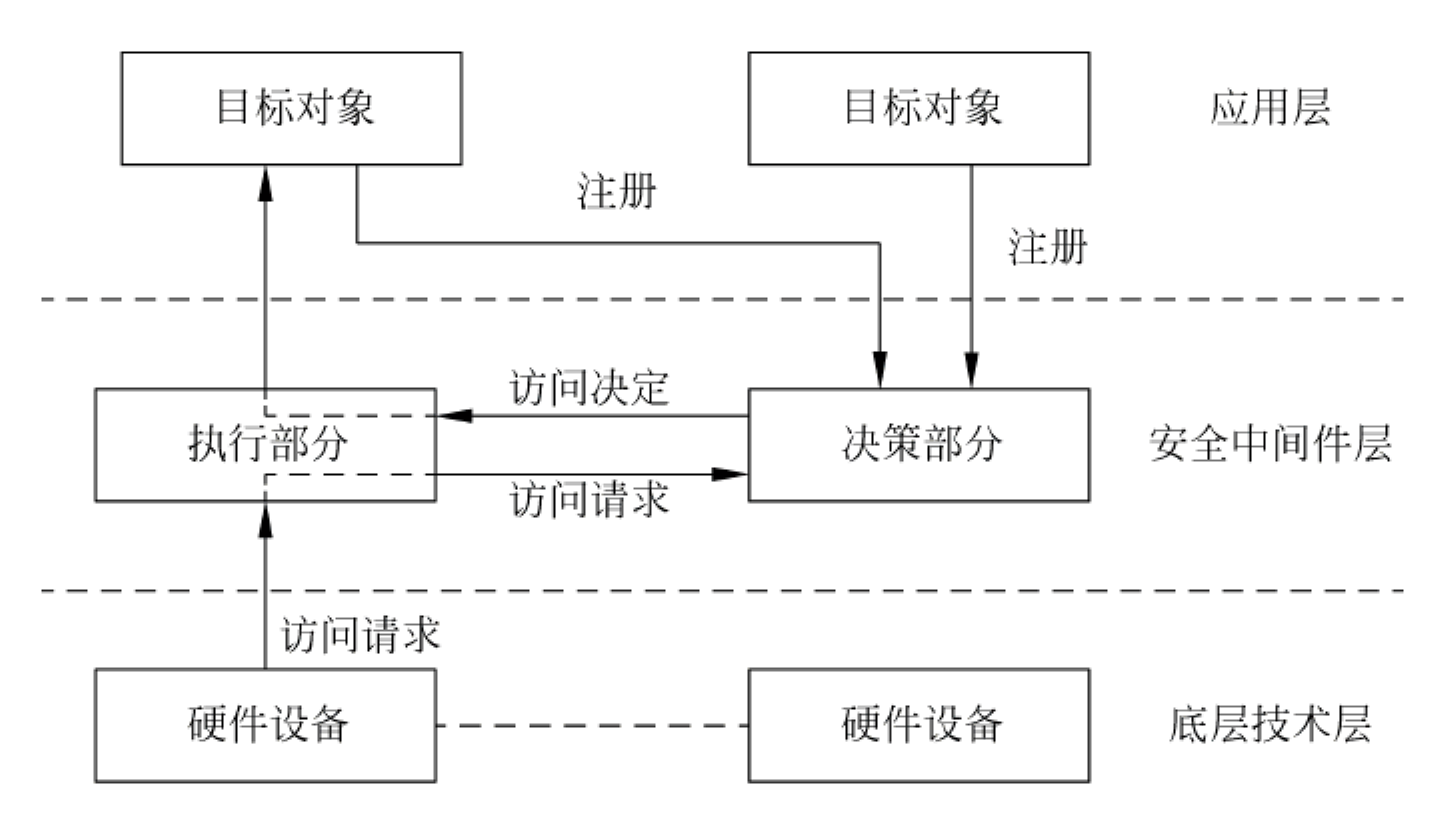


图 6-11 通用中间件安全模式

从图 6-11 中可以看出，决策部分给目标对象提供了接口，用于目标对象的注册。这是供应层对象调用的，用于获得目标对象的相关信息，从而提供安全策略，以辅助决策部分实现其功能。这个接口的实现；一方面有效地解决了对于应用层目标对象特定信息的访问控制；另一方面也是该模型对于应用层灵活性的体现，可以很容易地满足不同应用中不同的目标对象所要求的安全机制。

3. 基于中间件的物联网安全模型

中国学者姚远在 2011 年提出了一个基于中间件的物联网安全模型，认为物联网安全问题要从三个方面进行保护，即存储信息安全问题、传输安全问题和设备安全问题。

一般来说，中间件的设计应遵循整体的分层原则，中间件的设计框架如图 6-12 所示。

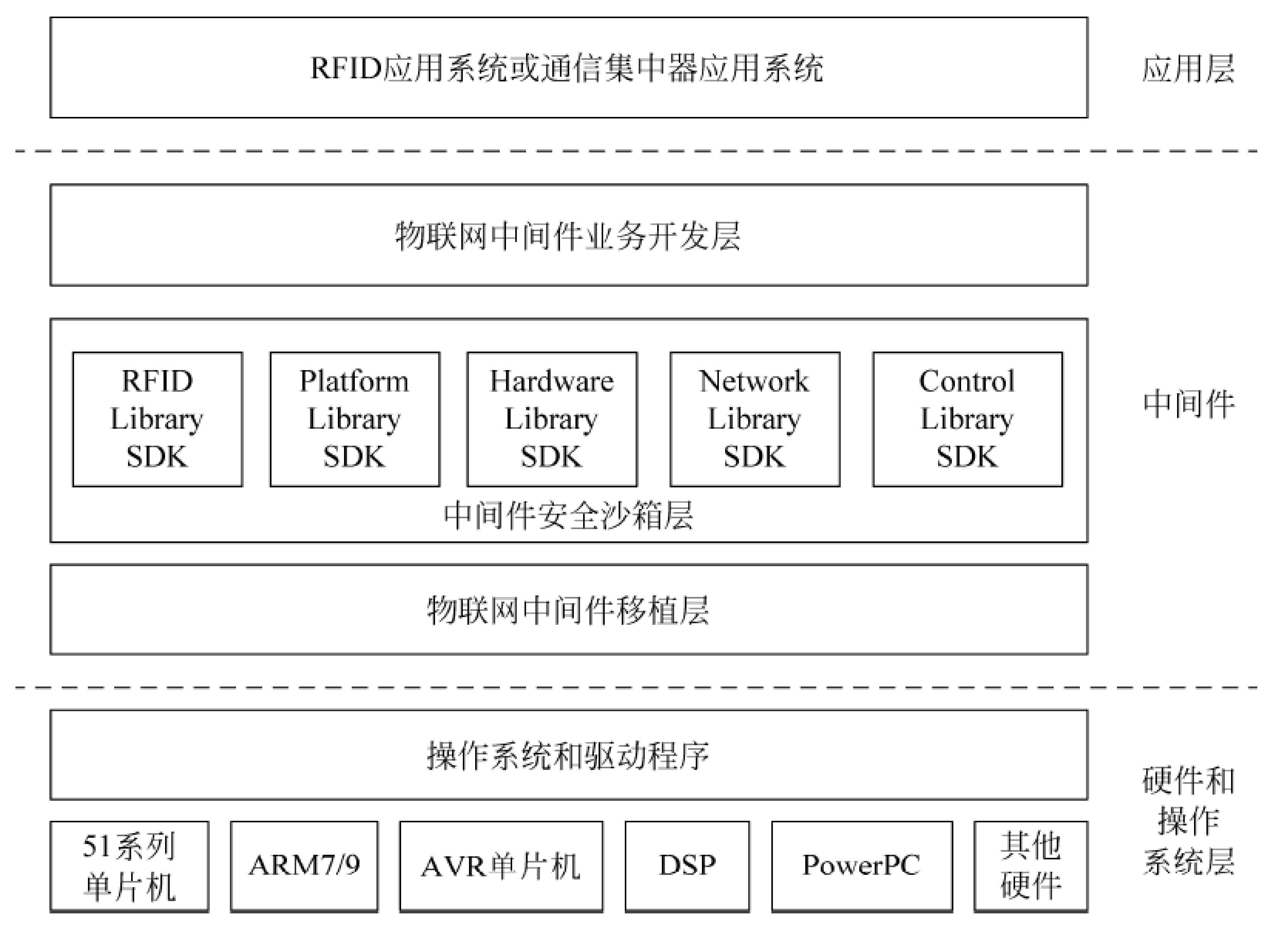


图 6-12 中间件框图

自下向上的第一层，是包含各种不同设备的硬件。这一部分的差异较大，从低端的单片机到高端的 DSP 数字信号处理器或者 PowerPC 通信处理器都会出现在这一层。

自下向上的第二层，是运行于各种硬件之上的软件环境层，这一部分的差异较硬件层小，通常由 Linux 和 Windows CE 等各种移动终端操作系统和驱动程序组成，其功能类似。

在图 6-12 中，中间最大的一块区域是中间件的实际范围。

1）移植层

移植层用作屏蔽底层差异，实现中间件的统一实施接口，同时也是平台的主要功能的体现接口。一般来说移植层的各种软硬件分别实现各自不同的功能，其接口包括线程或任务移植接口、显示移植接口、网络和通信移植接口、平台控制和属性移植接口、RFID 读写移植接口等。

2）安全沙箱层

中间件的关键模块是中间件安全沙箱层，其内部包含多种执行模块，如 RFID 模块、通信模块和硬件控制模块等，所有的模块统一位于一个安全沙箱中。该安全沙箱可以保证通信协议和远程控制对本地资源的安全访问。

沙箱（Sandbox）模型是一种保护本机安全的虚拟技术。利用沙箱技术，可以将系统关键数据进行虚拟化映射。外界对数据的获取和修正首先在沙箱映射层中实现。只有经过严格的授权才能访问底层实际硬件和资源，因此保证了设备本身不会受到病毒或恶意程序的

攻击造成崩溃。中间件中使用此模型时,通过远程调用和通信协议执行的一般信令,不可能访问真正的硬件设备资源。但是由于沙箱中的关键数据与系统中的数据时刻保持同步,沙箱模型并不会影响获取数据的实时性。

3）业务开发层

中间件的最上层是业务开发层,该层提供给本地或远程应用程序调用,以实现相应的业务功能。其接口设计一般包含物联网设备的控制,信息读写、通信、显示、授权认证等通用接口,并将这些模块的实现映射到安全沙箱中解析或执行。

物联网中间件从以下三个方面建立一个通用的安全模型:使用安全沙箱保证只有明确授权的应用程序才可以访问底层资源;支持基于 SSL、TSL 和 VPN 等加密通道传输信息;使用基于 X509 证书的授权方式保证终端和设备授权认证的通过。

中间件支持通过插件模式挂接不同的通信适配组件,如 SSL 安全层或 TSL 传输安全层,也可以配置及挂载 VPN 通道,实现数据的安全传输。传统的网络层加密机制是逐跳加密,即信息在发送过程中和传输过程中是加密的,但是在每个结点处却没有加密。

6.3 数据安全

6.3.1 数据安全概述

1. 数据安全的定义

数据安全也称为数据信息安全,是指数据在产生、传输、处理、存储等过程中的安全。换句话说,数据信息安全是指数据信息不受偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续、可靠、正常地运行,数据信息服务不中断。数据信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。数据信息安全包括的范围很广,大到国家军事政治等机密安全,小到如防范商业企业机密泄露、个人数据信息的泄露等。

进入网络时代后,数据信息安全保障工作的难度大大提高。我们受到日益严重的来自网络的安全威胁,诸如网络的数据窃贼、黑客的侵袭、病毒发布者,甚至系统内部的泄密者。数据信息安全已经成为各行业信息化建设中的首要问题。

随着“互联网＋”时代的到来,数据信息安全工作更是难上加难。据数据信息安全专家称,现有的搜索引擎已经有能力在 15 分钟内将全世界的网页存储一遍。换句话说,无论用加密账号,还是所谓的公司内网。只要你的信息被数据化,并与互联网接通,信息就已经自动进入失控状态,你将永远无法删除它,并且无从保密。

数据信息安全从来没有变得让人如此不安。数据信息安全技术作为一个独特的领域越来越受到各个行业的关注。

根据国际标准化组织的定义,数据安全的含义主要是指数据信息的完整性、可用性、保密性和可靠性。信息安全的内涵在不断地延伸,从最初的数据信息保密性发展到数据信息的完整性、可用性、可控性和不可否认性,进而又发展为“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。

数据安全的实质就是要保护信息系统或信息网络中的数据资源免受各种类型的威胁、干扰和破坏，即保证数据的安全性。

2. 数据安全的要素

数据安全的要素体现在以下 6 个方面。

1）保密性

保密性(Secrecy)，又称机密性，是指个人或团体的信息不被其他不应获得者获得。在电脑中，许多软件包括邮件软件、网络浏览器等，都有保密性相关的设定，用以维护用户资料的保密性，另外间谍档案或黑客也有可能会造成保密性的问题。

2）完整性

数据的完整性(Integrity)也称为可延展性(Malleably)，是信息安全的三个基本要点之一，它是指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现。在信息安全领域使用过程中，常常和保密性边界混淆。以普通 RSA 对数值信息加密为例，黑客或恶意用户在没有获得密钥破解密文的情况下，可以通过对密文进行线性运算，相应改变数值信息的值。例如交易金额为 X 元，通过对密文乘 2，可以使交易金额成为 2X。为解决以上问题，通常使用数字签名或散列函数对密文进行保护。

3）可用性

数据的可用性(Availability)是一种以使用者为中心的设计概念，易用性设计的重点在于让产品的设计能够符合使用者的习惯与需求。以互联网网站的设计为例，希望让使用者在浏览的过程中不会产生压力或感到挫折，并能让使用者在使用网站功能时，能用最少的努力发挥最大的效能。

4）可控性

可控性(Controllability)是指授权机构可以随时控制信息的机密性。“密钥托管”、“密钥恢复”等措施就是实现信息安全的可控性例子。

5）可靠性

可靠性(Reliability)是指信息能够在规定条件下和规定时间内完成规定操作的特性。可靠性是信息安全的最基本要求之一。

6）不可抵赖性

不可抵赖性也称不可否认性(Non-repudiation)，是指在信息交互过程中，确信参加者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接受的信息。

3. 威胁数据安全的因素

威胁数据安全的因素有很多，比较常见的主要有以下几个方面。

1）存储设备损坏

存储设备的物理损坏意味着数据丢失。设备的运行损耗、存储介质失效、运行环境以及人为的破坏等，都能给存储设备造成影响。

2）人为错误

由于操作失误，使用者可能会误删除系统的重要文件，或者修改影响系统运行的参数，以及没有按照规定要求或操作不当导致的系统宕机。

3）黑客

当入侵时，黑客通常通过网络远程入侵系统，侵入途径包括系统漏洞、管理不力等。

4）病毒

由于感染计算机病毒而使计算机系统受到破坏，造成的重大经济损失的事件屡屡发生，计算机病毒的复制能力强，感染性强，特别是网络环境下，传播更快。

5）数据信息窃取

从计算机上复制、删除数据信息甚至直接把计算机偷走。

4. 数据安全制度

数据安全制度的制订，一般要根据国家法律和有关规定制订适合本单位的数据安全制度，大致情况如下。

（1）对应用系统使用、产生的介质或数据，按其重要性进行分类，对存放有重要数据的介质，应备份必要份数，并分别存放在不同的安全地方（防火、防高温、防震、防磁、防静电及防盗），建立严格的保密保管制度。

（2）保留在机房内的重要数据（介质），应为系统有效运行所必需的最少数量，除此之外不应保留在机房内。

（3）根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。

（4）重要数据（介质）库，应设专人负责登记保管，未经批准，不得随意挪用重要数据（介质）。

（5）在使用重要数据（介质）期间，应严格按国家保密规定控制转借或复制，需要使用或复制的须经批准。

（6）对所有重要数据（介质）应定期检查，要考虑介质的安全保存期限，及时更新复制。损坏、废弃或过时的重要数据（介质）应由专人负责处理，秘密级以上的重要数据（介质）在过保密期或废弃不用时，要及时销毁。

（7）机密数据处理作业结束时，应及时清除存储器、联机磁带、磁盘及其他介质上有关作业的程序和数据。

（8）机密级及以上秘密信息存储设备不得并入互联网。重要数据不得外泄，重要数据的输入及修改应由专人来完成。重要数据的打印输出及外存介质应存放在安全的地方，打印出的废纸应及时销毁。

5. 数据技术

1）密码理论

密码理论是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，并将该规律应用于编制密码以保守通信秘密，我们称为编码学；应用于破译密码以获取通信情报，我们称为破译学，二者总称密码学。

2）数据加密

数据加密技术是最基本的网络安全技术，被称为信息安全的核心。最初主要用于保证

数据在存储和传输过程中的保密性，主要是通过各种方法将被保护信息置换成密文，然后再进行信息的存储或传输，即使加密信息在存储或传输过程为非授权人员所获得，也可以保证这些信息不为其认知，从而达到保护信息的目的。该方法的保密性直接取决于所采用的密码算法和密钥长度。

3）认证

相互认证是客户机和服务器相互识别的过程，它们的识别号使用公开密钥编码，并在SSL握手时交换各自的识别号。为了验证持有者是其合法用户，而不是冒名用户，SSL要求证明持有者在握手时对交换数据进行数字式标识。证明持有者要对包括证明的所有信息数据进行标识，以说明自己是证明的合法拥有者，这样就防止了其他用户冒名使用证明。证明本身并不提供认证，只有证明和密钥一起才起作用。

4）授权与访问控制

为了防止非法用户使用系统及合法用户对系统资源的非法使用，需要对计算机系统实体进行访问控制。对实体系统的访问控制必须对访问者的身份实施一定的限制，这是保证系统安全所必需的。要解决上述问题，访问控制需采取下述两种措施。

（1）识别与验证访问系统的用户。

（2）决定用户对某一系统资源可进行何种访问（读、写、修改、运行等）。

5）审计追踪

审计追踪是指对安防体系、策略、人和流程等对象的深入细致的核查，目的是为了找出安防体系中的薄弱环节并给出相应的解决方案。审计追踪的基本任务有两项：首先，检查实际工作是不是按照现有规章制度去办事的；其次，对审计步骤进行调整和编排，以便更好地判断出安防事件的发生地点或来源。

6）网间隔离与访问代理

从技术上来讲代理服务是一种网关功能，但它的逻辑位置是在OSI七层协议的应用层之上。代理使用一个客户程序与特定的中间结点链接，然后中间结点与期望的服务器进行实际链接。与应用网关型防火墙所不同的是，使用这类防火墙时外部网络与内部网络之间不存在直接连接，因此，即使防火墙产生了问题，外部网络也无法与被保护的网络连接。

7）反病毒技术

计算机病毒的预防、检测和清除是计算机反病毒技术的三大内容。也就是说计算机病毒的防治要从防毒、查毒和解毒三方面来进行；系统对于计算机病毒的实际防治能力和效果也要从防毒能力、查毒能力和解毒能力三方面来评判。防毒是指根据系统特性，采取相应的系统安全措施预防病毒侵入计算机；查毒是指对于确定的环境，能够准确地报出病毒名称；解毒是指根据不同类型病毒对感染对象的修改，并按照病毒的感染特性所进行的恢复，该恢复过程不能破坏未被病毒修改的内容，感染对象包括内存、引导区（含主引导区）、可执行文件、文档文件、网络等。

（1）防毒能力是指预防病毒侵入计算机系统的能力。

（2）查毒能力是指发现和追踪病毒来源的能力。

（3）解毒能力是指从感染对象中清除病毒，恢复被病毒感染前的原始信息的能力；解毒能力应用解毒率来评判。

8）入侵检测技术

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。入侵检测系统能够识别出来自于网络外部和内部的不希望有的活动。典型的入侵检测系统包括下述三个功能部件：

（1）提供事件记录流的信息源。

（2）发现入侵迹象的分析引擎。

（3）基于分析引擎的分析结果产生反映的响应部件。

6. 网络安全技术的综合利用

数据信息安全不仅是单一电脑的问题，也不仅是服务器或路由器的问题，而是整体网络系统的问题。所以信息安全要考虑整个网络系统，结合网络系统来制定合适的信息安全策略。由于网络安全涉及的问题非常多，如防病毒、防入侵破坏、防信息盗窃、用户身份验证等，这些都不是由单一产品来完成，也不可能由单一产品来完成，最重要的是，各种各样的单位产品堆砌依然无法给予数据信息安全完整的保护。数据信息安全也必须从整体策略来考虑，采用功能完善、技术强大的数据信息安全保障系统，例如SD-DSM系统等。这也是欧美国家近几年来数据信息安全技术领域研发的方向。

6.3.2　数据保护

1. 数据保护的概念

数据保护既是保证数据可用性，同样是保证业务连续性。数据保护的核心是建立和使用数据副本的技术。

随着互联网的发展，各企业、政府部门经历了数据量的爆炸性增长，数据正日益成为实际的资产，对任何组织来说，数据丢失都会带来严重的后果，甚至是灾难。

美国明尼苏达大学的研究报告指出：如果在发生数据丢失灾难后的两个星期内，无法恢复公司的业务系统，75%的公司业务将会完全停顿，43%的公司将再也无法开业。

2. 衡量数据保护的重要标准

衡量数据保护的重要标准有两个：

（1）恢复时间目标（Recovery Time Object，RTO），是指信息系统从灾难状态恢复到可运行状态所需要的时间，用来衡量容灾系统的业务恢复能力。

（2）恢复点目标（Recovery Point Object，RPO），是指业务系统所允许的在灾难过程中的最大数据丢失量，用来衡量容灾系统的数据冗余备份能力。

3. 数据保护技术实现的层次与分类

数据保护技术涉及设备、网络、系统和应用四个层次。在设备层，主要有备份和复制技术；在网络层，随着对备份系统容量和速度的需求越来越高，附网存储（NAS）、存储区域网（SAN）已逐渐取代了传统的直连存储（DAS）；在系统层，主要是镜像技术、快照技术和连续

数据保护技术；在应用层，典型的有数据库备份技术。数据的持续增长和应用的高连续性对备份性能的要求越来越高，未来该领域尚有待于在数据去重、备份验证、I/O优化、节能技术等方面进行更深入的研究。

数据保护技术主要分为三大类：备份技术、镜像技术和快照技术。

1）备份技术

备份技术就是将数据加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用进行系统恢复的一个过程。

数据备份与数据恢复是保护数据的最后手段，也是防止信息攻击的最后一道防线。数据备份的根本目的是重新利用，备份工作的核心是恢复。一个无法恢复的备份，对任何系统来说都是毫无意义的。另外，数据备份的意义不仅在于防范意外事件的破坏，而且还是历史数据保存归档的最佳方式。

（1）备份策略。

数据备份要根据实际情况来制定不同的备份策略。目前被采用最多的备份策略主要有以下三种。

① 全备份(full backup)：是对数据的完全备份。

② 增量备份(incremental backup)：是对上次全备份或者增量备份后被修改了的文件做备份。

③ 差分备份(differential backup)：是备份自上次全备份后被修改过的文件。

在实际应用中，备份策略通常是以上三种的结合。例如每周一至周六进行一次增量备份或差分备份，每周日进行全备份，每月底进行一次全备份，每年底进行一次全备份。

（2）数据备份模式。

数据备份有LAN备份、LAN Free备份和SAN Server-Free备份等三种备份模式。LAN备份针对所有存储类型都可以使用，LAN Free备份和SAN Server-Free备份只能针对SAN架构的存储。

① 基于LAN备份。

传统备份需要在每台主机上安装磁带机备份本机系统，采用LAN备份策略，在数据量不是很大时候，可采用集中备份。一台中央备份服务器将会安装在LAN中，然后将应用服务器和工作站配置为备份服务器的客户端。中央备份服务器接受运行在客户机上的备份代理程序的请求，将数据通过LAN传递到它所管理的、与其连接的本地磁带机资源上。这一方式提供了一种集中的、易于管理的备份方案，并通过在网络中共享磁带机资源提高效率。

② LAN-Free备份。

由于数据通过LAN传播，当需要备份的数据量较大，备份时间紧迫时，网络容易发生堵塞。在SAN环境下，可采用存储网络的LAN-Free备份，需要备份的服务器通过SAN连接到磁带机上，在LAN-Free备份客户端软件的触发下，读取需要备份的数据，通过SAN备份到共享的磁带机。这种独立网络不仅可以使LAN流量得以转移，而且它的运转所需的CPU资源低于LAN方式，这是因为光纤通道连接不需要经过服务器的TCP/IP栈，而且某些层的错误检查可以由光纤通道内部的硬件完成。在许多解决方案中需要一台主机来管理共享的存储设备以及用于查找和恢复数据的备份数据库。

③ SAN Server-Free 备份。

LAN Free 备份需要占用备份主机的 CPU 资源，如果备份过程能够在 SAN 内部完成，而大量数据流无须流过服务器，则可以极大地降低备份操作对服务器硬件系统的影响。SAN Server-Free 备份就是这样的技术。

2）镜像技术

数据镜像技术如图 6-13 所示，就是通过同样的 I/O 读写操作，在独立的 2 个存储区域（通常是逻辑卷）中保存相同的数据，并且可以同时进行 I/O 读写操作。

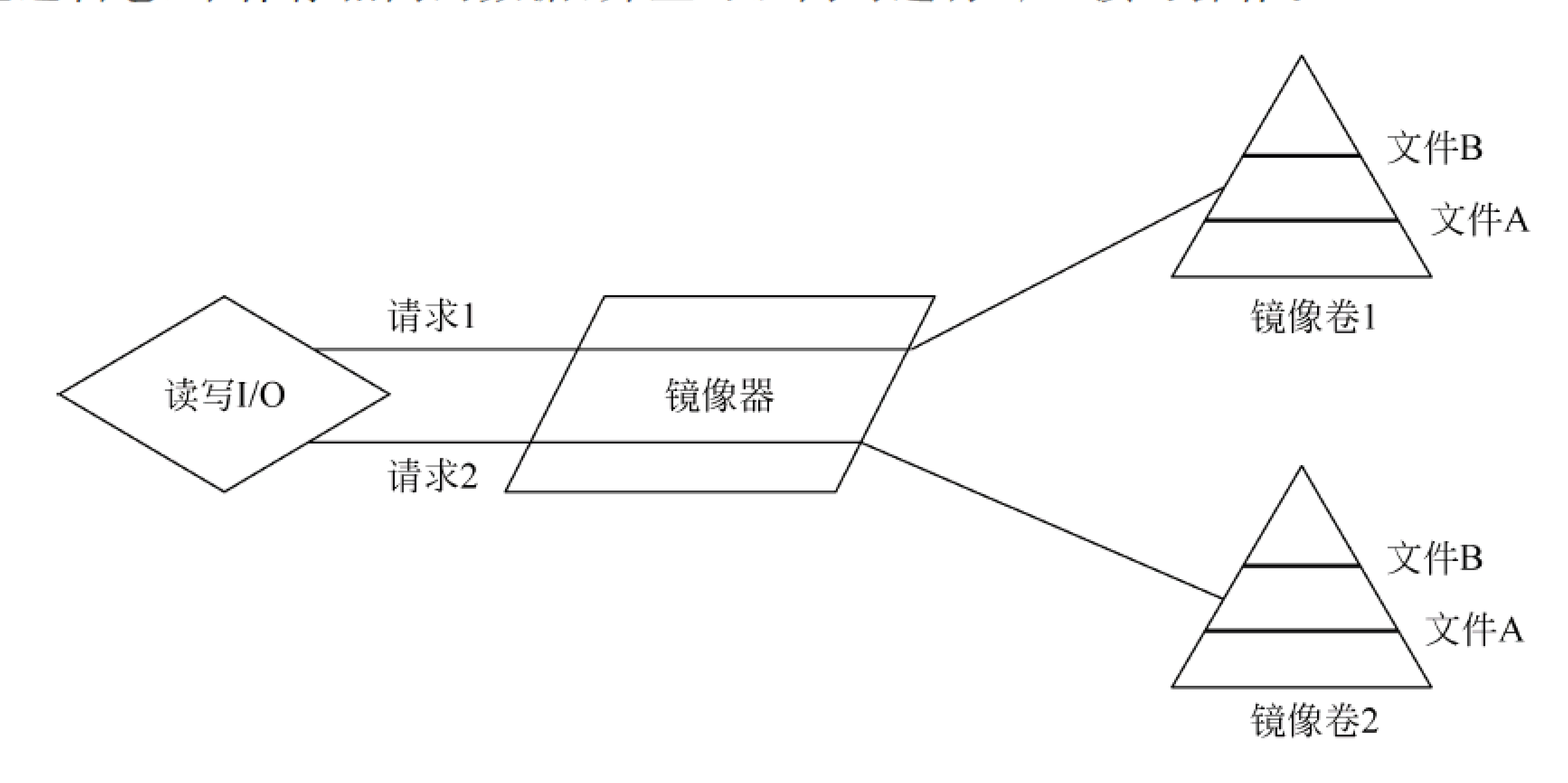


图 6-13 对数据的镜像读写

（1）镜像的工作模式。

数据镜像包括一个主镜像系统和一个从镜像系统。按主、从镜像存储系统所处的位置可分为本地镜像和远程镜像。远程镜像按请求镜像的主机是否需要镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

同步远程镜像数据的每一个“写”操作会同时在主镜像卷和从镜像卷上完成，主镜像卷的“写”操作完成后，还需要等待从镜像卷完成“写”操作，才能进行下一个 I/O 操作。数据随机写入，每一个 I/O 操作需等待主镜像卷和从镜像卷都完成，确认信息方可释放，要求存储主镜像设备和从镜像设备的性能保持一致，一般用于要求数据零丢失、严格的数据一致性的关键场所。

异步远程镜像虽然同时将“写”命令和数据同时发送给主镜像卷和从镜像卷，但主镜像卷的“写”操作完成后并不需要等待从镜像卷完成“写”操作，从镜像卷的“写”操作可以通过数据复制进程异步完成。数据每个 I/O 顺序写入缓存(Cache)，再由缓存随机写入主镜像卷和从镜像卷；系统只须等待写缓存的确认信息。主镜像设备和从镜像设备的性能可以不同，一般用于对于性能要求高，允许少量数据丢失的重要应用。

（2）卷镜像复制和 RAID 镜像卷。

卷镜像复制工作方式的系统结构如图 6-14 所示。

根据两个存储设备之间工作方式的不同，数据同步和复制机制的不同，可分为两种方式，第一种是卷镜像复制方式，第二种是 RAID 镜像卷方式。

左侧为主存储设备，右侧为备用存储设备，再通过卷镜像复制软件、数据备份软件、网络层的存储虚拟化设备、存储设备自带的卷镜像复制功能等多种方式来实现主、备两个存储之

间的卷镜像复制,以此来保障数据的安全性。同时备份存储设备也可以作为数据存储服务功能的一种后备方式,一旦主存储设备发生故障,就需要自动或手动的切换到备份存储设备上。

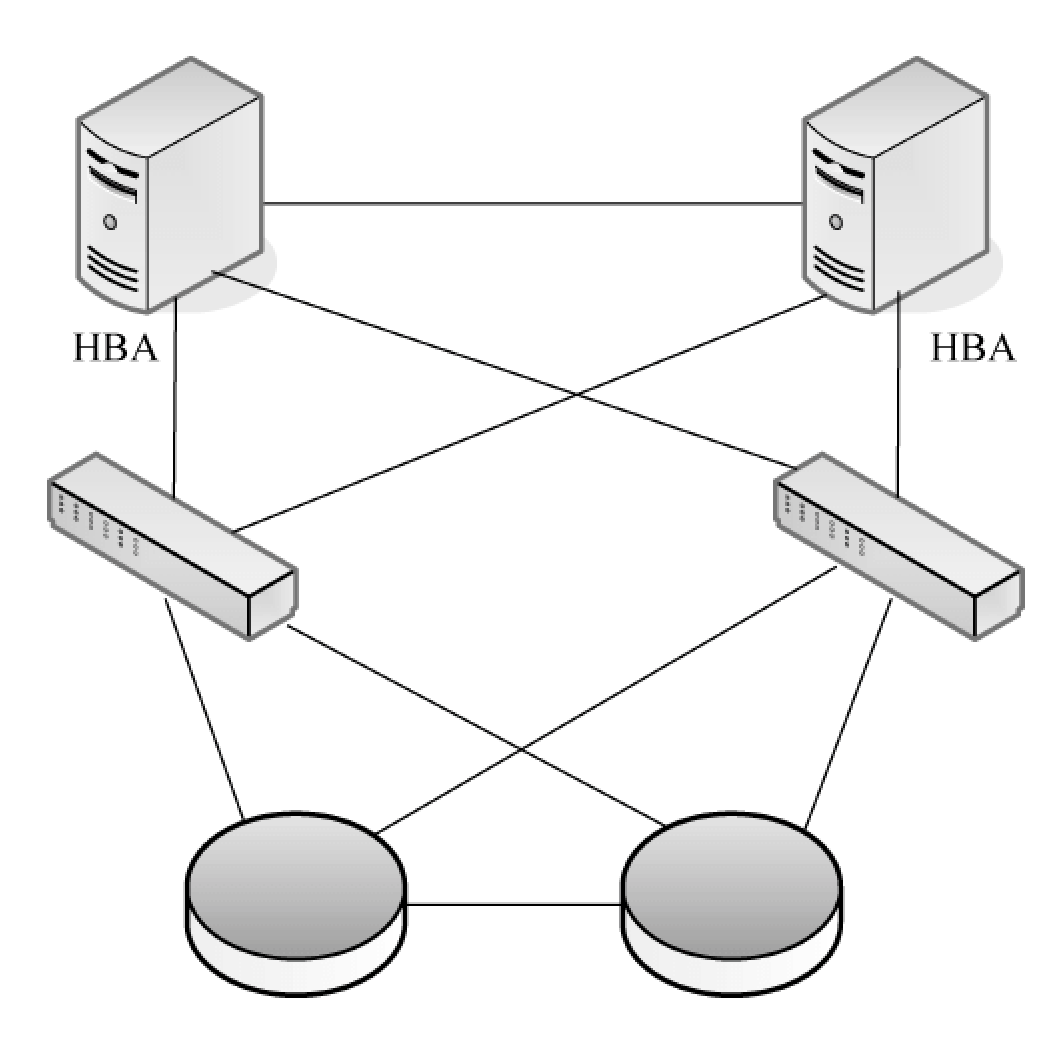


图 6-14 卷镜像复制工作方式的系统结构图

RAID 卷镜像工作方式的系统结构如图 6-15 所示。

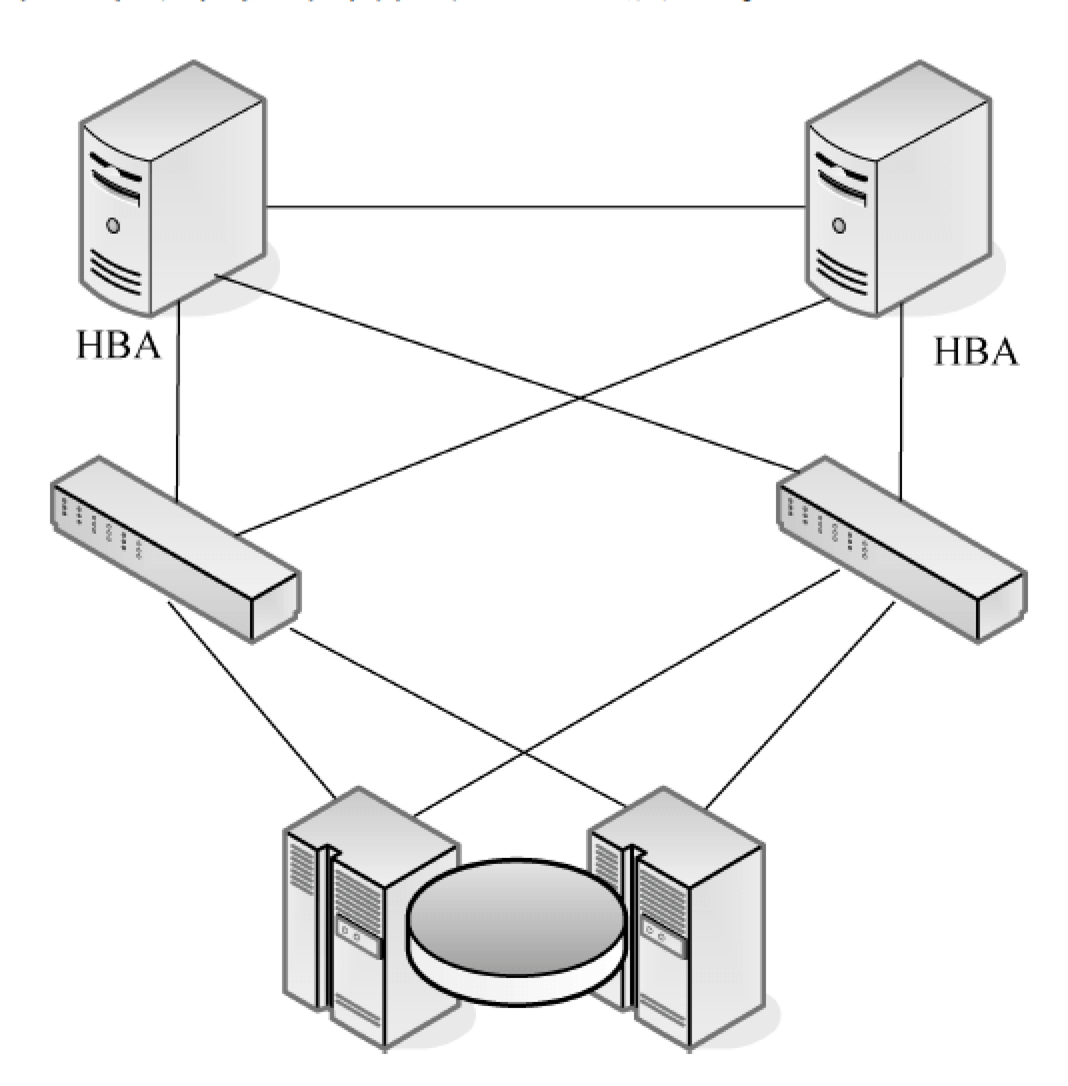


图 6-15 RAID 卷镜像复制工作方式的系统结构图

两台存储设备之间可以是跨越一个存储设备的 RAID 镜像卷,数据库服务器主机对该镜像卷进行数据读写操作。由于 RAID 镜像卷跨越两个存储设备,因此一台存储设备发生整体故障,RAID 镜像卷都不会发生故障,也不会影响数据库服务器端业务的正常进行。

与图 6-14 相比,图 6-15 中的存储设备对外提供的是一个镜像卷,而不是两个卷。当一个存储设备发生故障时,不需要在两个卷进行切换,主机端不需要加载新卷,数据库服务器也不需要重新启动。

在图 6-15 系统中,两台存储设备通过控制器内含集群功能,创建了一个 RAID 镜像卷,实现双机工作的方式,从而使得整个数据库存储系统达到了主机、软件、网络和存储等所有层面的双机冗余高可用。

(3) 卷镜像复制功能实现。

根据数据库系统的网络结构图可以将数据库系统分成三层,即主机层、网络层和存储设备层,如图 6-16 所示。卷镜像复制在不同层有不同的实现方式。

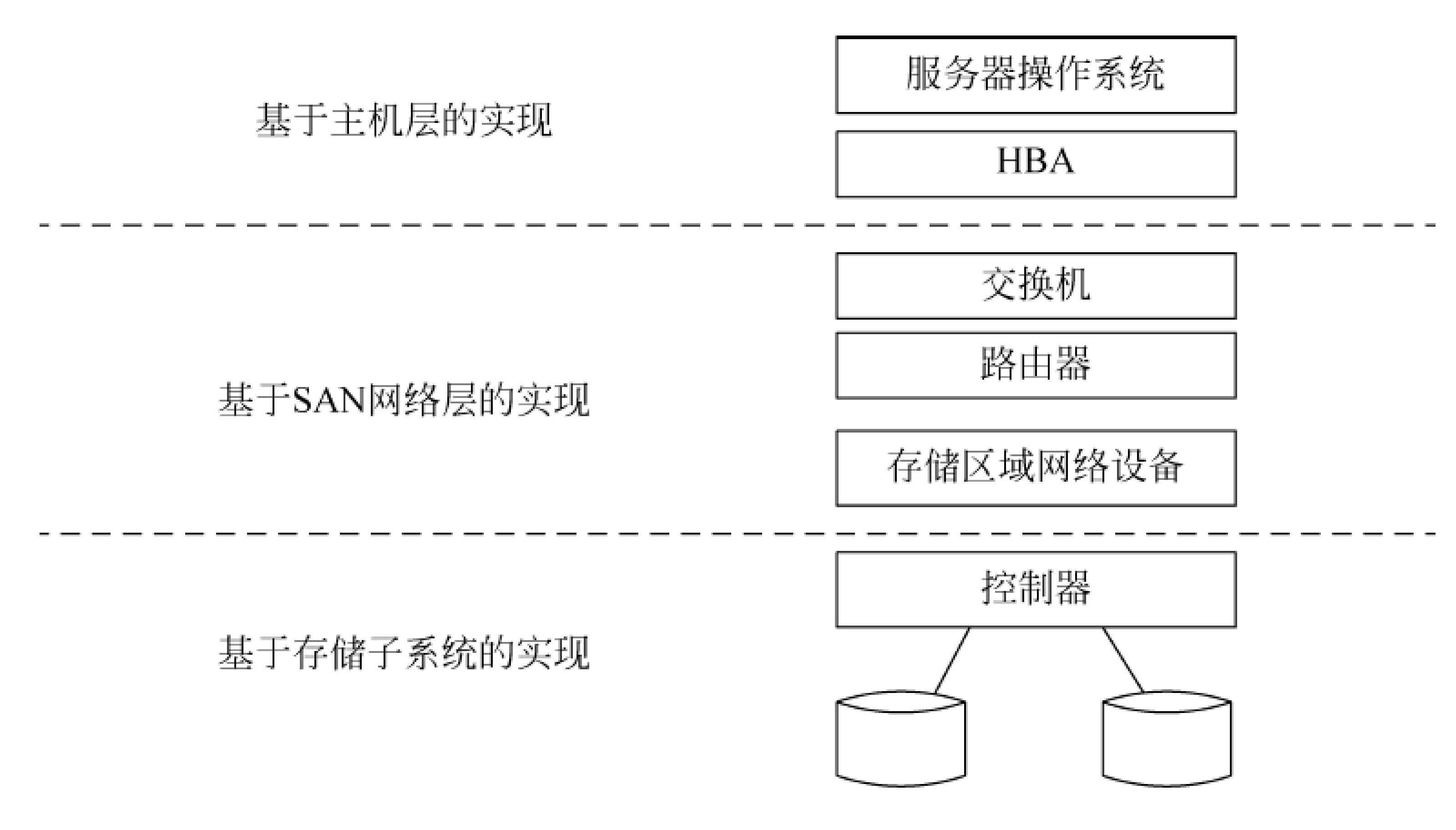


图 6-16　卷镜像复制在不同层有不同的实现方式

① 主机层实现卷镜像复制。

主机层实现卷镜像复制是指在主机上实现卷镜像管理和卷复制的软件,并依靠软件来实现数据在两个卷之间的同步或复制。典型的软件如:Veritas Volume Replication。

在主机层实现卷镜像复制方式中,数据先写入一个卷,然后由软件再定时复制到备份卷内,或直接由软件同步写入到两个卷。主机层实现卷镜像复制的系统结构如图 6-17 所示。

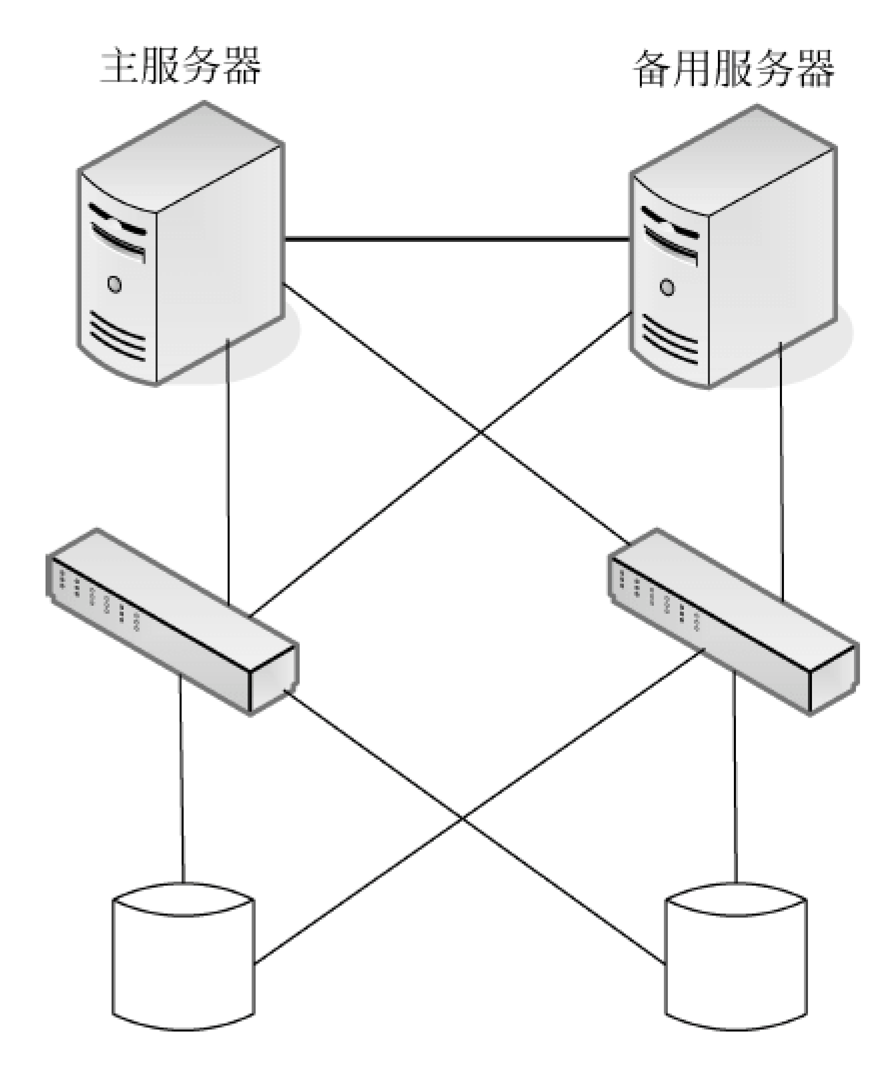


图 6-17　主机层实现卷镜像复制

这种方式的缺点是数据同步操作由软件实现，占用主机资源和网络资源非常大。当一个存储发生在实际应用中经常会出现问题，一个存储设备发生故障时，主机端并不能正常地启用另一个存储。

② 智能存储层实现卷镜像复制。

许多中高端的智能型存储设备，如 EMC Symmetrix 系列、IBM ESS 系列、HP XP512 系列、HDS 9900 系列和 UIT BM6800 系列产品，都可以通过 ShadowImage、SRDF、Timefinder、Flashcopy 或 TrueCopy、Remote Volume Mirror 等功能实现卷镜像复制功能。分别位于不同存储设备上的两个卷之间建立卷复制镜像功能，存储设备控制器自动将写入主卷的数据复制到备份卷中。当主存储设备发生故障时，业务将会切换到备用存储设备上，并启用备份卷，保证数据库业务不会中断，数据不会丢失，其结构如图 6-18 所示。

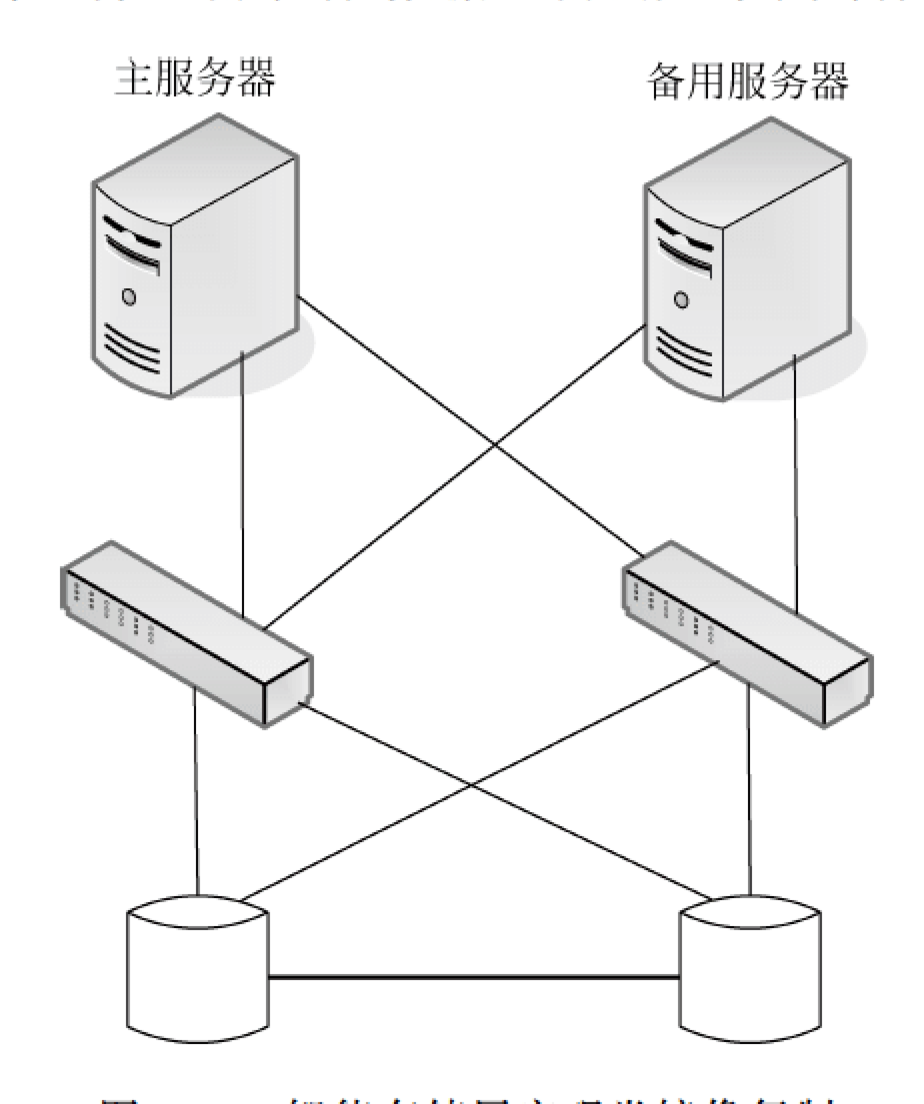


图 6-18 智能存储层实现卷镜像复制

这种方式的优点是数据复制和镜像功能在存储设备内部由控制器来完成，不需要主机或第三方软件的参与，数据复制进程安全稳定，安装调试及维护简单。缺点是卷镜像复制进程占用存储设备的资源非常大。主备存储切换时，必须先断开两个卷之间的镜像复制关系，才能启动备份卷。主机在切换主、备份卷的过程中必须停止数据库服务，引起业务中断。整个切换时间较长，一般需要 10～30 分钟，根据无法满足数据库系统所要求的 99.99%的高可用性。

③ 网络层实现卷镜像复制。

网络层的数据复制或镜像功能一般是由网络层的存储虚拟化设备来实现，这种方式的特点是依靠外加的网络层设备来实现两个存储设备之间的数据复制，数据复制过程不占用主机资源，两个存储之间的数据同步在网络层完成。根据存储虚拟化设备工作机制的不同，一般来说，可以分为带内（In-Band）和带外（Out-of-Band）两种。

如图 6-19 所示为常见的带内的存储虚拟化设备的实现卷镜像复制的系统结构图。

存储虚拟化设备分别连接主机端虚拟化（Fabric）和存储端虚拟化，其主要功能是管理对存储设备上的逻辑卷，对已有逻辑卷进行虚拟化或创建虚拟的条带卷，消除存储设备异构

对主机系统的影响，提高存储设备的可用性和总体性能。另外一个功能就是卷复制和镜像，通过存储虚拟化设备实现两个虚拟卷之间的数据安全保护。

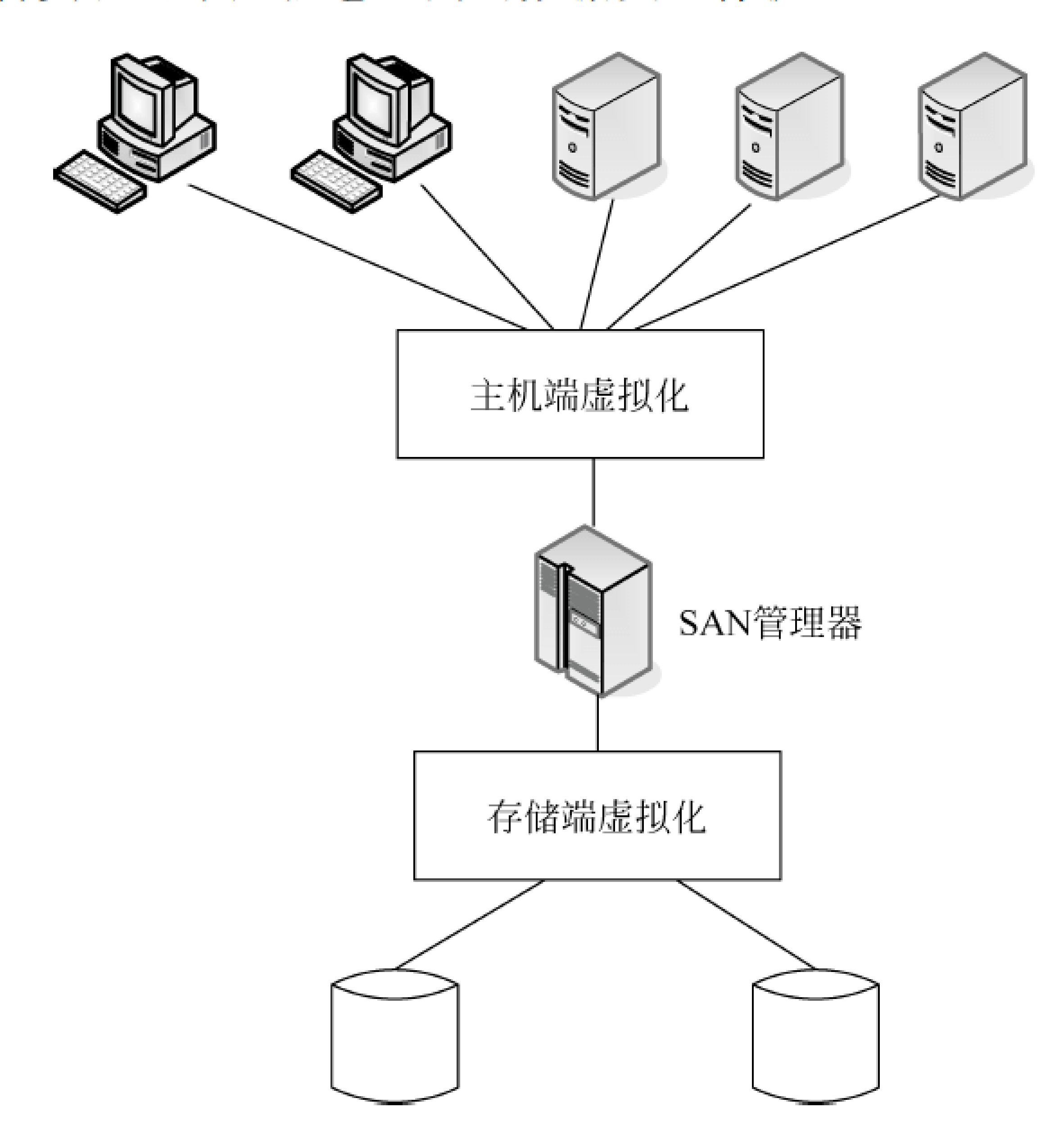


图 6-19　带内存储虚拟化设备的系统结构

如图 6-20 所示为常见的带外存储虚拟化设备的系统结构图。存储虚拟化设备所提供的功能也类似。

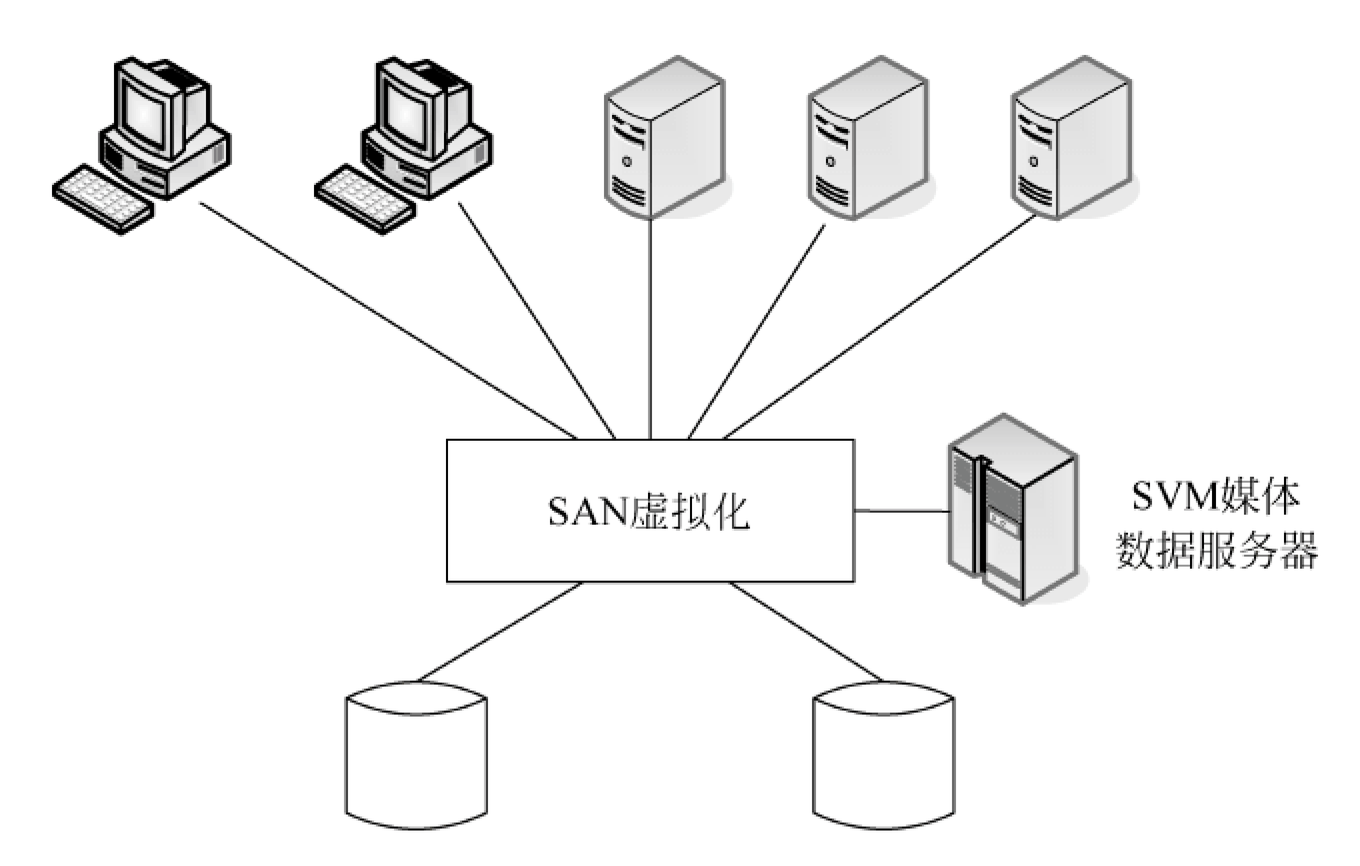


图 6-20　带外存储虚拟化设备的系统结构

通过存储虚拟化设备实现卷镜像复制功能的优势在于操作由存储虚拟化设备来完成、压力集中的存储虚拟化设备上，不需要主机参与，数据复制进程安全稳定。缺点是需要增加专用存储虚拟化设备，带外方式有的需要在主机端需要安装存储虚拟化设备的客户端软件，比如 UIT SVM，有的需要依赖高端智能交换机，比如 EMC VSM。而带内方式虚拟化设备则极易成为整个系统的性能瓶颈和故障点。

网络层的数据复制主要依靠快照来实现，由于两次快照之间有时间间隔，因此两个存储

设备之间的数据并不是完全同步的，一旦主存储设备发生故障，即使能启用备用存储，也有可能丢失一个快照周期的数据。

(4) RAID 镜像卷功能实现分析。

RAID 镜像卷一般有两种实现方式，一是在主机层由卷管理软件来实现；二是在存储层通过存储设备集群来实现。

① 主机层实现镜像卷。

一般来说，主机层的镜像卷功能都是由安装在主机上的卷管理软件来实现的，例如用 Veritas Volume Manager 这个软件来实现。

主机层实现 RAID 镜像卷的结构如图 6-21 所示。

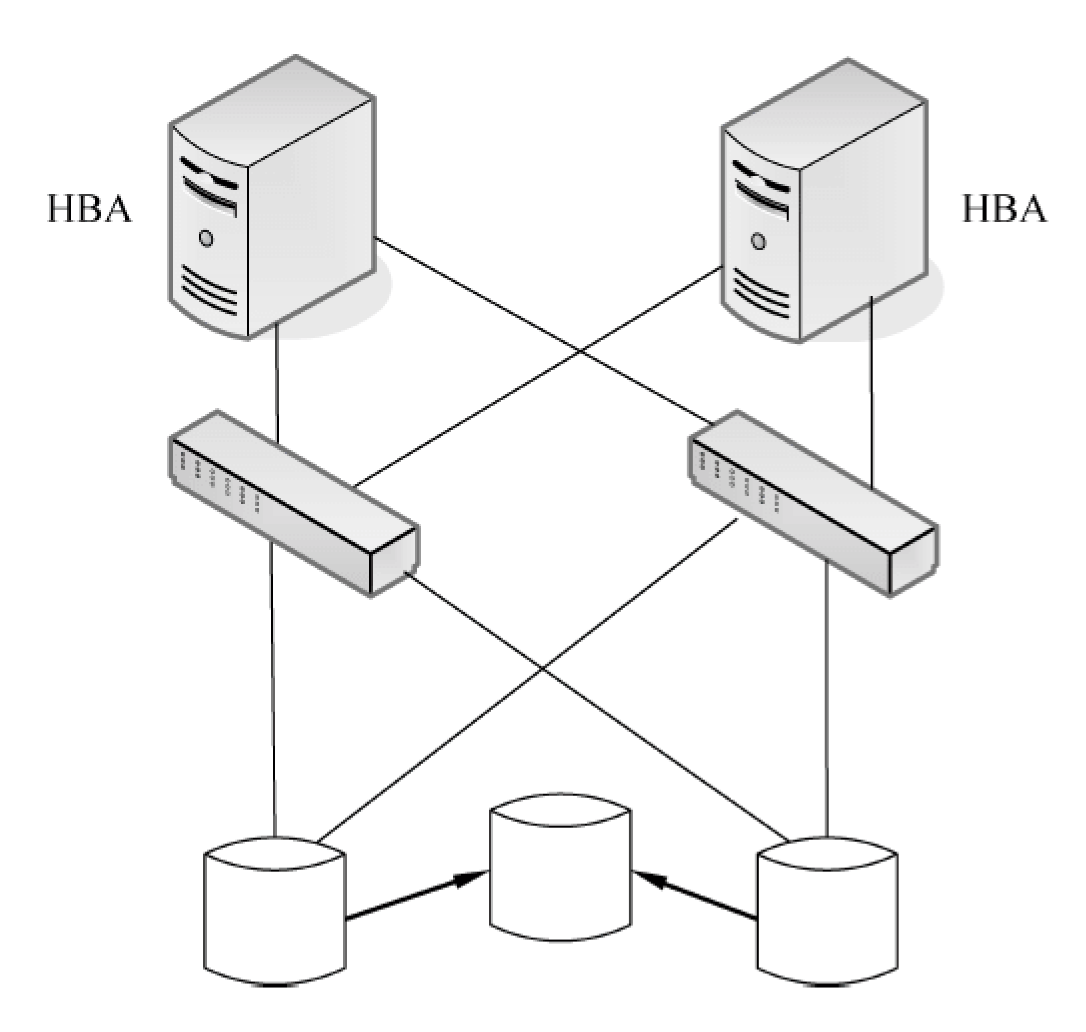


图 6-21 主机层实现 RAID 镜像卷

在图 6-21 中，两个存储设备分别创建两个容量和参数相同的卷，映射给数据库主机，卷管理软件用这两个卷创建一个软 RAID1 的镜像卷。这样当数据库写入数据时，数据按照 RAID1 的机制会同步写入两个存储系统，并保证两个存储系统间数据的同步和一致性。

这种实现方式的缺点镜像卷由卷管理软件来实现，卷的长期安全性和稳定性无法保障。卷管理软件占用主机资源非常大，且会随着存储设备、网络层或 HBA 卡发生故障而大幅度增加，极易引起数据库死机。很多实际应用证明了这个实现方式在大型的数据库系统中是非常不稳定的。

② 存储层实现镜像卷。

存储层实现 RAID 镜像卷的结构如图 6-22 所示。存储设备层的镜像功能一般是指通过存储设备自身强大的集群功能，跨存储设备创建镜像卷。镜像卷由两个存储设备的控制器共同管理，数据同步写入两个存储设备。

这种方式的特点是两个存储设备的控制器以集群方式工作，共同管理镜像卷，主机端识别到的只是一个镜像卷，而不是前三种方式中识别到的两个卷。因此即使是任何一个存储设备发生整体瘫痪，镜像卷都不会出现故障或报错，主机端也不会发生逻辑卷“丢失”、报错或需要进行切换，当然更不需要重新启动数据库服务。

镜像功能由存储设备层实现，数据同步写入两个存储设备，不需要主机或任何客户端软

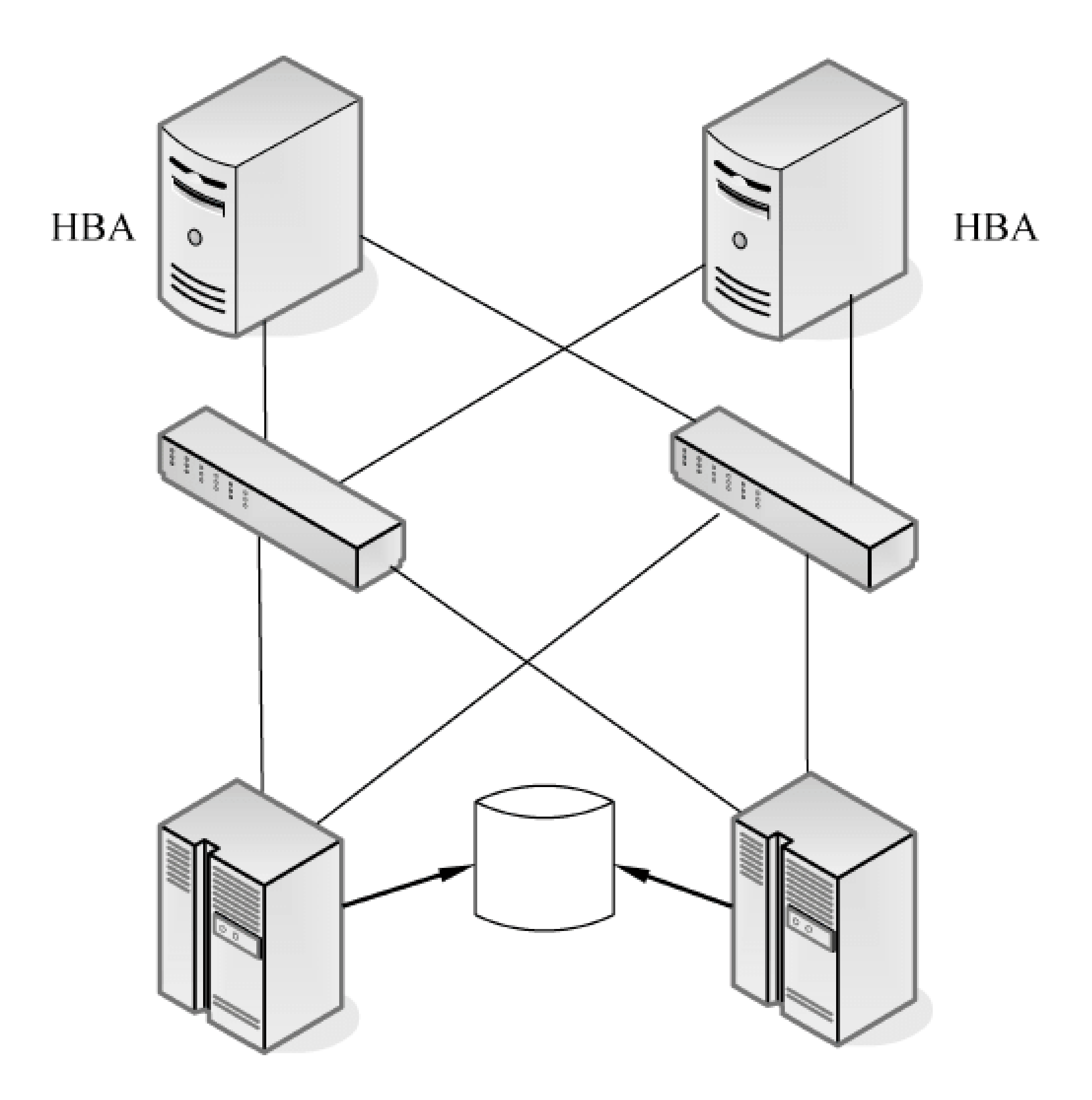


图 6-22　存储层实现 RAID 镜像卷

件的参与，因此不会占用网络层或主机资源。

3）快照技术

快照是关于指定数据集合的一个完全可用复制，该复制包括相应数据在某个时间点（复制开始的时间点）的映像。快照可以是其所表示的数据的一个副本，也可以是数据的一个复制品。

（1）快照技术分类。

快照技术分为两大类，一类称为即写即复制（copy-on-write）快照；另一类称为分割镜像快照。

① 即写即复制快照.

即写即复制快照可以在每次输入新数据，或已有数据被更新时生成对存储数据改动的快照。这样做可以在发生硬盘写错误、文件损坏或程序故障时迅速地恢复数据。但是，如果需要对网络或存储媒介上的所有数据进行完全的存档或恢复时，所有以前的快照都必须可供使用。

即写即复制快照表现在数据外观的特征是“照片”。这种方式通常也被称为“元数据”复制，即所有的数据并没有被真正复制到另一个位置，只是指示数据实际所处位置的指针被复制。在使用这项技术的情况下，当已经有了快照时，如果有人试图改写原始的存储设储上的数据，快照软件将首先将原始的数据块复制到一个新位置（专用于复制操作的存储资源池），然后再进行写操作。以后当你引用原始数据时，快照软件将指针映射到新位置，或者当你引用快照时将指针映射到老位置。

② 分割镜像快照。

分割镜像快照引用镜像硬盘组上所有数据。每次应用运行时，都生成整个卷的快照，而不只是新数据或更新的数据。这就使离线访问数据成为可能，并且简化了恢复、复制或存档一块硬盘上的所有数据的过程。但是，这是个较慢的过程，而且每个快照需要占用更多的存储空间。

分割镜像快照也叫作原样复制，由于它是某一个逻辑单元号(Logical Unit Number，LUN)或文件系统上的数据的物理复制，有的管理员称之为克隆、映像等。原样复制的过程可以由主机(Windows 上的 MirrorSet、Veritas 的 Mirror 卷等)或在存储级上用硬件完成(Clone、BCV、ShadowImage 等)。

(2) 实现快照的方法。

具体实现快照的方法，可以分为三种：冷快照复制、暖快照复制和热快照复制。

① 冷快照复制。

进行冷快照复制是保证系统可以被完全恢复的最安全的方式。在进行任何大的配置变化或维护过程之前和之后，一般都需要进行冷复制，以保证完全的恢复原状(rollback)。冷复制还可以与克隆技术相结合复制整个服务器系统，以实现各种目的，如扩展、制作服务器系统的副本供测试/开发之用以及向二层存储迁移。

② 暖快照复制。

暖快照复制利用服务器的挂起功能。当执行挂起行动时，程序计数器被停止，所有的活动内存都被保存在引导硬盘所在的文件系统中的一个临时文件(.vmss 文件)中，并且暂停服务器应用。在这个时间点上，进行整个服务器(包括内存内容文件和所有的 LUN 以及相关的活动文件系统)的快照复制。在这个复制中，机器和所有的数据将被冻结在完成挂起操作时的处理点上。

当快照操作完成时，服务器可以被重新启动，在挂起行动开始的点上恢复运行。应用程序和服务器过程将从同一时间点上恢复运行。从表面上看，就好像在快照活动期间按下了一个暂停键一样。对于服务器的网络客户机看来，就好像网络服务暂时中断了一下一样。对于适度加载的服务器来说，这段时间通常在 30～120 秒。

③ 热快照复制。

在这种状态下，发生的所有的写操作都立即应用在一个虚硬盘上，以保持文件系统的高度的一致性。服务器提供让持续的虚拟硬盘处于热备份模式的工具，以通过添加重做(REDO)日志文件在硬盘子系统层上复制快照复制。

一旦 REDO 日志被激活，复制包含服务器文件系统的 LUN 的快照是安全的。在快照操作完成后，可以发出另一个命令，这个命令将 REDO 日志处理提交给下面的虚拟硬盘文件。当提交活动完成时，所有的日志项都将被应用，REDO 文件将被删除。在执行这个操作过程中，会出现处理速度的略微下降，不过所有的操作将继续执行。但是，在多数情况下，快照进程几乎是瞬间完成的，REDO 的创建和提交之间的时间非常短。

热快照操作过程从表面上看基本上察觉不到服务器速度下降。在最差情况下，它看起来就是网络拥塞或超载的 CPU 可能造成的一般服务器速度下降。在最好情况下，不会出现可察觉到的影响。快照技术都是在应用层或文件层实现的，在备份的过程中开销较大，应用范围也相对较窄。

4. 持续数据保护技术

持续数据保护技术(Continuous Data Protection，CDP)是数据保护领域的一项重大突破。传统的数据保护解决方案都将主要精力放在定期的数据备份上。但是，在定期备份状态下一直伴随有备份窗口、数据一致性以及对服务器系统的影响等问题。而 CDP 技术，则

将注意力的焦点从备份转向了恢复。它可以为重要数据中的变化提供连续的保护，IT 管理员根本不需要考虑备份的问题。当灾难发生时，基于 CDP 的解决方案可以迅速恢复到任何一个需要的还原点，从而为用户提供更大的灵活性和更高的性能。

1）CDP 的概念

SNIA 数据保护论坛（DMF）的持续数据保护特别兴趣小组（CDP SIG）对 CDP 的定义是，持续数据保护是一套方法，它可以捕获或跟踪数据的变化，并将其在数据之外独立存放，以确保数据可以恢复到过去的任意时间点。持续数据保护系统可以基于块、文件或应用实现，能够为恢复对象提供足够细的恢复粒度，实现几乎无限多的恢复时间点。

SNIA 给出的概念中明确指出了 CDP 技术可以"确保数据能恢复到过去的任意时间点"，因此可以提供较以往更为灵活的目标恢复点（Recovery Point Objectives，RPO）和更快的目标恢复时间（Recovery Time Objectives，RTO）。它可以捕获和保护数据中所有的变化，而非仅仅是某个预先选定的时间点，这样就可以随时访问数据，减少数据损失并消除代价高昂的停机损失，同时数据的检索也变得非常可靠、快速和精细。

2）CDP 的实现方式

实现持续数据保护的关键就是对数据变化的记录和保存，实现在任意时间点的快速恢复。它一般有三种实现方式：基准参考数据模式、合成参考数据模式和复制参考数据模式。

（1）基准参考数据模式。

我们先来看一下基准参考数据模式的工作原理：首先，根据已产生的数据来建立供恢复时用的参考数据复制（这个复制只需建立一次）；其次，在参考数据复制的基础上向前顺序记录数据变化事件日志；最后，当需要对某些数据恢复时，便根据数据变化事件日志，在参考数据复制的基础上完成恢复操作。

基准参考数据模式的工作原理如图 6-23 所示。

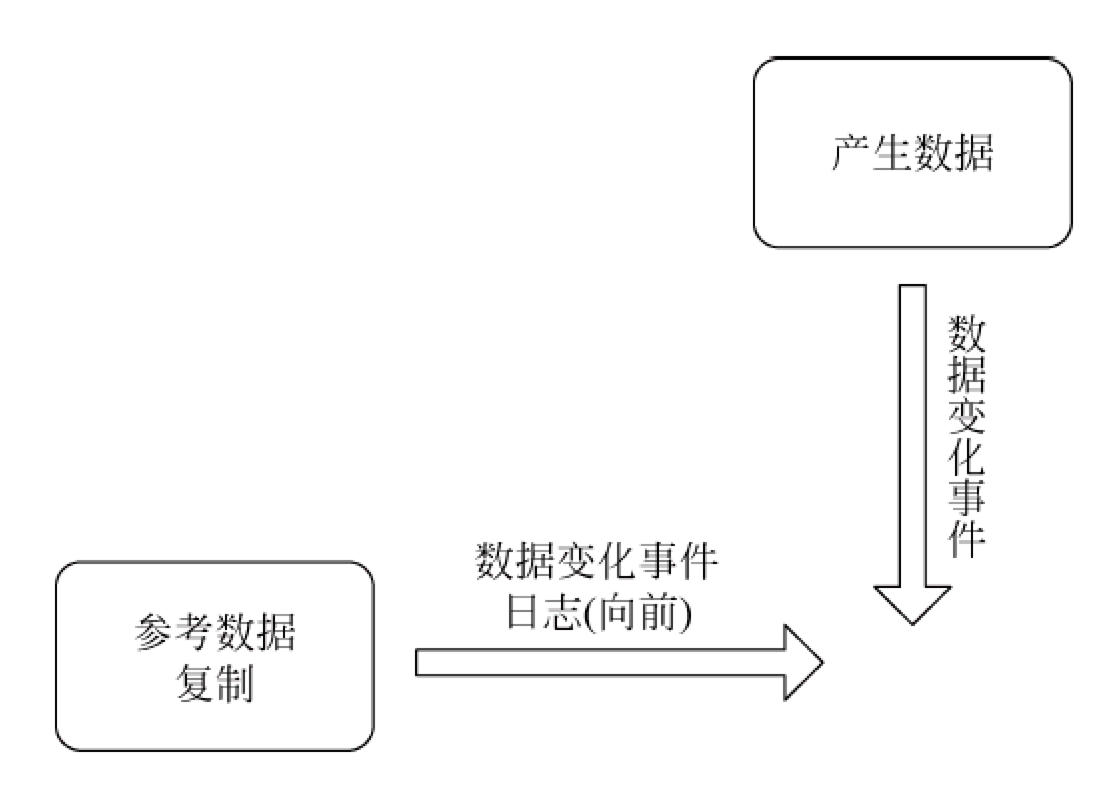


图 6-23　基准参考数据模式

从图 6-23 可以看出，基准参考数据模式原理简单，实现起来也较容易，但由于数据恢复时需要从最原始的参考数据开始，依次进行数据恢复，所以恢复时间较长。特别是越靠近当前的恢复时间点，恢复所需要的时间就越长。

（2）复制参考数据模式。

复制参考数据模式的工作原理如图 6-24 所示。

首先，在原始数据产生的同时，恢复时所需的参考数据也同时产生；其次，在同步产生

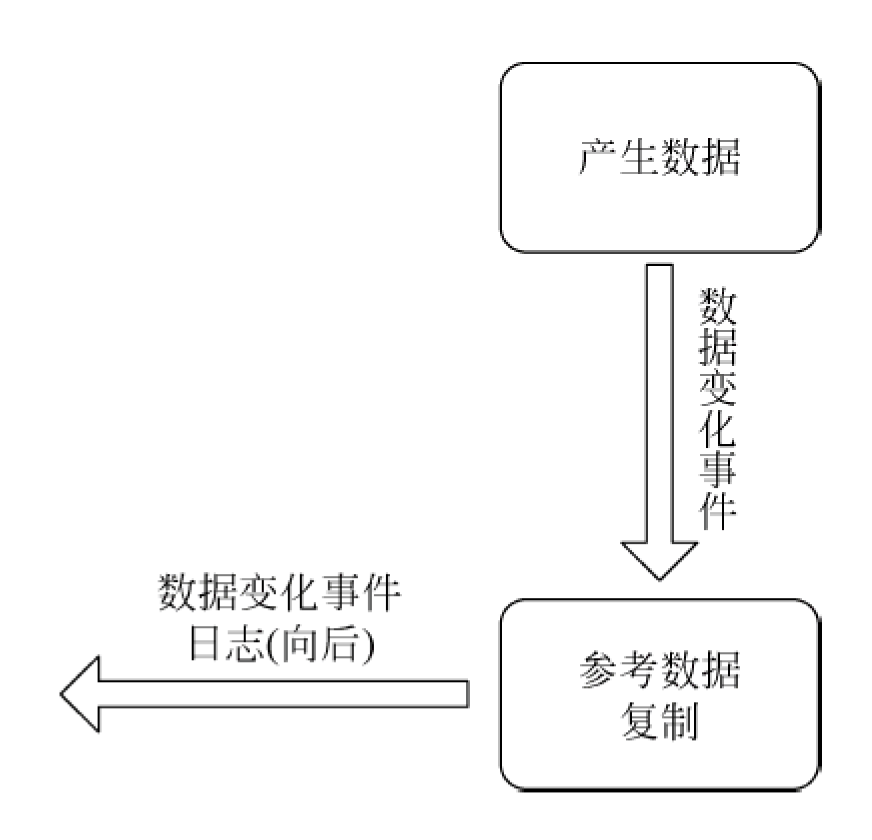


图 6-24　复制参考数据模式

参考数据复制的同时，数据变化事件日志便以当前所产生的数据为基础，回退记录以前数据的变化情况；最后，当需要恢复时，则在当前数据的基础上，依据变化日志，回退到过去任意时间点。

比较图 6-23 与图 6-24 可以看出，复制参考数据模式与基准参考数据模式在实现原理上是相反的。复制参考数据模式在数据恢复时，恢复的时间点越靠近当前，所需要的恢复时间就越短。但是在数据的保存过程中，它需要同时进行数据和日志记录的同步，因此需要较多的系统资源。

（3）合成参考数据模式。

合成参考数据模式的工作原理：首先，同基准参考数据模式一样，建立参考数据复制和顺序向前记录的数据变化事件日志；其次，定期根据前一次的参考数据复制和变化事件日志，对最初的参考数据复制向前移动，使参考数据复制记录的是当前产生的数据，而数据变化日志也变成回退记录以前数据的变化情况；最后，在需要恢复的时候，就可以像复制参考模式那样进行了。

合成参考数据模式的工作原理如图 6-25 所示。

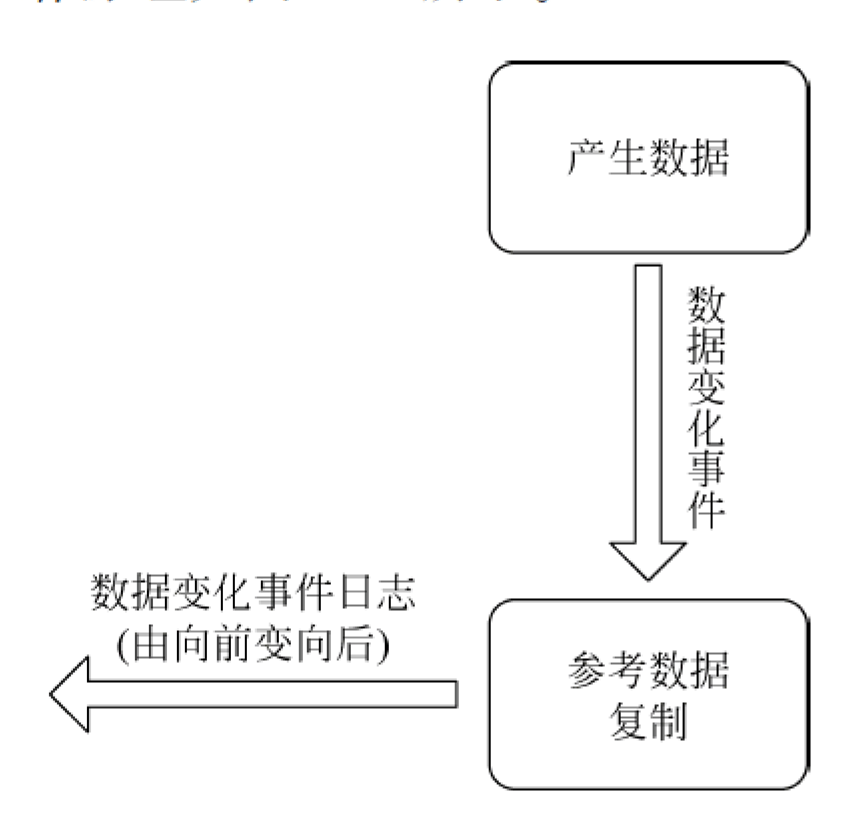


图 6-25　合成参考数据模式

通过图 6-25 我们可以看出，合成参考数据模式是基准参考数据模式和复制参考数据模式的折中，它可以得到较好的资源占用和恢复时间效果。但是，它的实现是需要复杂的软件

管理和数据处理功能,因此真正实现起来还是比较复杂的。

3) CDP 的分类

从操作方式来看,CDP 解决方案的设计方法可以分为基于块的,基于文件的和基于应用的。因此,CDP 的实现模式也可分为以下三种。

(1) 基于数据块实现的 CDP。

基于数据块实现的 CDP,它的功能是直接运行在物理存储设备或逻辑卷管理器上的,甚至也可以运行在数据传输层上。当数据块写入生产数据的主存储设备时,CDP 系统可以捕获数据的副本,并将其存放在另外一个存储设备中。它的实现方式又可分为三类:基于主机层、基于传输层和基于存储层。

(2) 基于文件实现的 CDP。

基于文件实现的 CDP,作用在文件系统之上。它可以捕捉文件系统数据或者元数据的变化事件(例如文件的创建、修改、删除等),并及时将文件的变动进行记录,以便将来实现任意时间点的文件恢复。

(3) 基于应用实现的 CDP。

基于应用实现的 CDP,直接位于受保护的特定应用之中。对需要保护的关键应用程序,可以在其中直接嵌入和运行 CDP 功能。这种实现方式能够和应用进行深度整合,确保应用数据在持续保护中的一致性。此外,它作为应用自身的内置功能,也可以利用特殊的应用 API 在发生变化时赋予其连续访问应用内部状态的权限。它最大的好处就是与应用程序结合紧密,管理比较灵活,便于用户部署和实施。

通过上述的介绍,我们可以看出基于块和基于文件的 CDP,可以利用一种相同的通用方法来支持多种不同的应用。而基于应用的 CDP 则只为某种应用提供持续数据保护功能,但它的表现形式则是一种更为深入的集成方式。

4) CDP 技术的应用

虽然 CDP 技术是近几年兴起的新技术,但是它已经逐渐被人们运用到了实际工作中。

(1) 因为 CDP 技术的恢复时间(RTO)和恢复点(RPO)的粒度更细,所以,CDP 技术对于当前数据的备份会更及时,而对数据的恢复则更具有随意性。特别是在备份、恢复那些变化较快的数据,如备份、恢复邮件服务器中的电子邮件信息时,CDP 技术比传统数据备份技术更具优势。因此,它在这方面的应用较为广泛。

(2) CDP 技术的应用可以使数据的丢失量尽可能的少,因此它也应用于对关键数据的备份和恢复。

CDP 技术目前已经成为备份领域中最为热点的技术,存储业的生产商也纷纷推出这方面的产品,其中包括来自 IBM 公司的文件级 CDP 软件产品(IBM Tivoli Continuous Data Protection for Files)、来自 HP 和 EMC 的块级 CDP、来自 Mendocino 软件以及来自微软和 Symantec(赛门铁克)的快照和复制工具。总之,随着人们对 CDP 技术关注程度的提高,在不久的将来,它一定会得到更为广泛的应用。

6.3.3 数据库保护

1. 数据库保护概述

为了适应和满足数据共享的环境和要求,DBMS 要保证整个系统的正常运转,防止数

据意外丢失和不一致数据的产生，以及当数据库遭受破坏后能迅速地恢复正常，这就是数据库的保护。

数据库保护又叫做数据库控制，是通过四个方面实现的，即安全性控制、完整性控制、并发性控制和数据恢复。

数据库的安全性是保护数据库，以防止因非法使用数据库而造成的数据泄露、更改或破坏。

数据库的完整性是保护数据库中的数据的正确性、有效性、相容性。

并发控制是为了防止多个用户同时存取同一数据，造成的数据不一致。

数据恢复将因破坏或故障而导致的数据库中数据的错误状态恢复到最近一个正确状态的技术。

2. 威胁数据库的安全因素

数据库系统中的数据由 DBMS 统一管理与控制，为了保证数据库中数据的安全、完整和正确有效，要求对数据库实施保护，使其免受某些因素影响从而对其中数据造成的破坏。

一般地说，对数据库的破坏来自以下 4 个方面：

1）非法用户

非法用户是指那些未经授权而恶意访问、修改甚至破坏数据库的用户，包括那些超越权限来访问数据库的用户。一般地说，非法用户对数据库的危害是相当严重的。

2）非法数据

非法数据是指那些不符合规定或语义要求的数据，一般由用户的误操作引起。

3）各种故障

各种故障指的是各种硬件故障（如磁盘介质）、系统软件与应用软件的错误、用户的失误等。

4）多用户的并发访问

数据库是共享资源，允许多个用户并发访问（Concurrent Access），由此会出现多个用户同时存取同一个数据的情况。如果对这种并发访问不加控制，各个用户就可能存取到不正确的数据，从而破坏数据库的一致性。

3. 数据库安全保护措施

针对以上 4 种对数据库破坏的可能情况，数据库管理系统（DBMS）核心已采取相应措施对数据库实施保护，具体如下：

1）利用权限机制

只允许有合法权限的用户存取所允许的数据，这就是“数据库安全性”应解决的问题。

2）利用完整性约束

防止非法数据进入数据库，这是“数据库完整性”应解决的问题。

3）提供故障恢复（Recovery）能力

保证各种故障发生后，能将数据库中的数据从错误状态恢复到正确状态，这是“故障恢复技术”的内容。

4）提供并发控制（Concurrent Control）机制

控制多个用户对同一数据的并发操作，以保证多个用户并发访问的顺利进行，这是“并

发控制”的内容。

4. 数据库安全性机制

数据库的安全性是指在信息系统的不同层次保护数据库,防止未授权的数据访问,避免数据的泄漏、不合法的修改或对数据的破坏。安全性问题不是数据库系统所独有的,它来自各个方面,其中既有数据库本身的安全机制,如用户认证、存取权限、视图隔离、跟踪与审查、数据加密、数据完整性控制、数据访问的并发控制、数据库的备份和恢复等方面,也涉及计算机硬件系统、计算机网络系统、操作系统、组件、Web 服务、客户端应用程序、网络浏览器等。只是在数据库系统中大量数据集中存放,而且为许多最终用户直接共享,从而使安全性问题更为突出,每一个方面产生的安全问题都可能导致数据库数据的泄露、意外修改、丢失等后果。

一般地说,在计算机系统中,安全措施是一级接着一级地设置的,数据库系统安全的模型如图 6-26 所示。

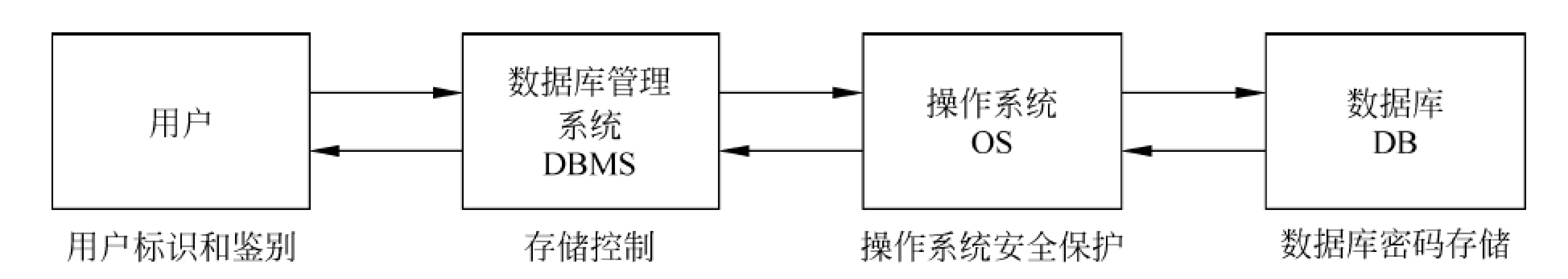


图 6-26　数据库系统安全的模型

在图 6-26 的安全模型中,用户要进入计算机系统,系统首先根据输入的用户标识进行用户身份鉴定,只有合法的用户才准许进入计算机系统。对已经进入系统的用户,DBMS 要进行存取控制,只允许用户执行合法操作。操作系统一级也会有自己的保护措施。数据最后还可以以密码形式存储在数据库中。

在本节中,对数据库的一些逻辑安全机制进行介绍,包括用户认证、存取控制,视图隔离、数据加密、审查等内容作介绍。

1) 用户认证

数据库系统不允许一个未经授权的用户对数据库进行操作。用户标识与鉴别,即用户认证,是系统提供的最外层安全保护措施。其方法是由系统提供一定的方式让用户标识自己的名字或身份,每次用户要求进入系统时,由系统进行核对,通过鉴定后才提供机器使用权。对于获得上机权的用户若要使用数据库时,数据库管理系统还要进行用户标识和鉴定。

用户标识和鉴定的方法有很多种,而且在一个系统中往往多种方法并用,以得到更强的安全性。常用的方法是用户名和口令。

通过用户名和口令来鉴定用户的方法简单易行,但其可靠程度极差,容易被他人猜出或测得。因此,设置口令法对安全强度要求比较高的系统不适用。近年来,一些更加有效的身份认证技术迅速发展起来。例如使用某种计算机过程和函数、智能卡技术,物理特征(指纹、声音、笔迹等)认证技术等具有高强度的身份认证技术日益成熟,并取得了不少应用成果,为将来达到更高的安全强度打下了坚实的理论基础。

2）存取控制

数据库安全性所关心的主要是 DBMS 的存取控制机制。数据库安全最重要的一点就是确保只授权给有资格的用户访问数据库的权限，同时令所有未被授权的人员无法接近数据，这主要通过数据库系统的存取控制机制实现。存取控制是数据库系统内部对已经进入系统的用户的访问控制，是安全数据保护的前沿屏障，是数据库安全系统中的核心技术，也是最有效的安全手段。

在存取控制技术中，DBMS 所管理的全体实体分为主体和客体两类。主体（Subject）是系统中的活动实体，包括 DBMS 所管理的实际用户，也包括代表用户的各种进程。客体（Object）是存储信息的被动实体，是受主体操作的，包括文件、基本表、索引和视图等。

数据库存取控制机制包括两个部分：

（1）定义用户权限，并将用户权限登记到数据字典中。用户权限是指不同的用户对不同的数据对象允许执行的操作权限。系统必须提供适当的语言定义用户权限，这些定义经过编译后存放在数据字典中，被称作系统的安全规则或授权规则。

（2）合法性权限检查。当用户发出存取数据库的操作请求后（请求一般应包括操作类型、操作对象、操作用户等信息），数据库管理系统查找数据字典，根据安全规则进行合法权限检查，若用户的操作请求超出了定义权限，系统将拒绝执行此操作。

3）视图隔离

视图是数据库系统提供给用户以多种角度观察数据库中数据的重要机制，是从一个或几个基表（或视图）导出的表，它与基表不同，是一个虚表。数据库中只存放视图的定义，而不存放视图对应的数据，这些数据仍存放在原来的基本表中。

从某种意义上讲，视图就像一个窗口，透过它可以看到数据库中自己感兴趣的数据及其变化。进行存取权限控制时，可以为不同的用户定义不同的视图，把访问数据的对象限制在一定的范围内。也就是说，通过视图机制要把保密的数据对无权存取的用户隐藏起来，从而对数据提供一定程度的安全保护。

需要指出的是，视图机制最主要的功能在于提供数据独立性，在实际应用中，常常将视图机制与存取控制机制结合起来使用，首先用视图机制屏蔽一部分保密数据，再在视图上进一步定义存取权限。通过定义不同的视图及有选择地授予视图上的权限，可以将用户、组或角色限制在不同的数据子集内。

4）数据加密

前面介绍的几种数据库安全措施，都是防止从数据库系统中窃取保密数据。但数据存储在存盘、磁带等介质上，还常常通过通信线路进行传输，为了防止数据在这些过程中被窃取，妥当的方法是对数据进行加密。对于高度敏感性数据，例如财务数据、军事数据、国家机密，除了上述安全措施外，还必须采用数据加密技术。有关加密技术的知识请阅读本书第 3 章。

加密的基本思想是根据一定的算法将原始数据（术语为明文）变换为不可直接识别的格式（术语为密文），从而使得不知道解密算法的人无法获知数据的内容。数据解密是加密的逆过程，即将密文数据转变成可见的明文数据。

一个密码系统包含明文集合、密文集合、密钥集合和算法，其中密钥和算法构成了密码系统的基本单元。算法是一些公式、法则或程序，它规定明文与密文之间的变换方法，密钥

可以看作算法中的参数。

密码系统的结构如图 6-27 所示。

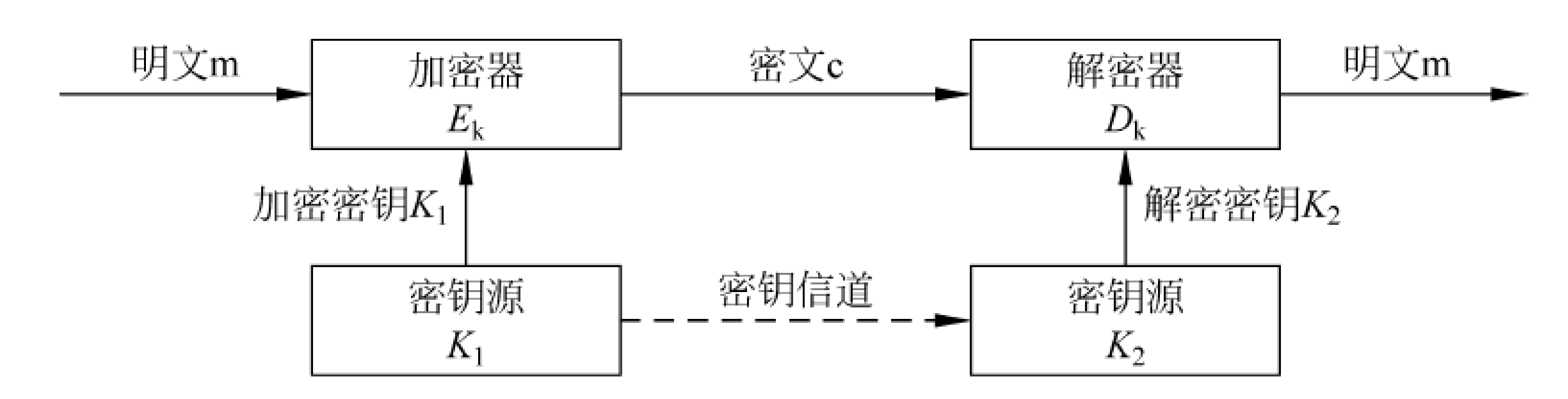


图 6-27 数据加密系统

加密方法可分为对称加密与非对称加密两种。

所谓对称加密，其加密所用的密钥与解密所用的密钥相同。典型的代表是 DES(Data Encryption Standard)数据加密标准。所谓非对称加密，其加密所用的密钥与解密所用的密钥不相同，其中加密的密钥可以公开，而解密的密钥不可以公开。

数据加密和解密是相当费时的操作，其运行程序会占用大量系统资源，因此数据加密功能通常是可选特征，允许用户自由选择，一般只对机密数据进行加密。

5) 审计

审计功能是 DBMS 达到 C2 级以上安全级别必不可少的指标。这是数据库系统的最后一道安全防线。

审计功能把用户对数据库的所有操作自动记录下来，存放在日志文件中。DBA 可以利用审计跟踪的信息，重现导致数据库现有状况的一系列事件，找出非法访问数据库的人、时间、地点以及所有访问数据库的对象和所执行的动作。

一般地说，有两种审计方式，即用户审计和系统审计。

(1) 用户审计：DBMS 的审计系统记下所有对表或视图进行访问的企图(包括成功的和不成功的)及每次操作的用户名、时间、操作代码等信息。这些信息一般都被记录在数据字典(系统表)之中，利用这些信息用户可以进行审计分析。

(2) 系统审计：由系统管理员进行，其审计内容主要是系统一级命令以及数据库客体的使用情况。

审计通常是很费时间和空间的，所以 DBMS 往往将其作为可选特征，一般主要用于安全性要求较高的部门。

5. 数据库的完整性机制

1) 概述

数据库的完整性机制是防止合法用户使用数据库时向数据库中加入不符合语义的数据，完整性措施的防范对象是不合语义的数据。

数据库的安全性和完整性是数据库安全保护的两个不同的方面。数据库的安全性保护数据库以防止不合法用户故意造成的破坏，而数据库的完整性则保护数据库以防止合法用户无意中造成的破坏。从数据库的安全保护角度来讲，完整性和安全性是密切相关的。

数据库完整性的基本含义是指数据库中数据的正确性、有效性和相容性，指数据库中数

据与现实世界的实际情况是相符的或数据库中数据自身不存在自相矛盾的现象。其主要目的是防止错误的数据进入数据库。正确性是指数据的合法性，例如数值型数据只能含有数字而不能含有字母。有效性是指数据是否属于所定义域的有效范围。相容性是指表示同一事实的两个数据应当一致，不一致即是不相容。

数据库管理系统的完整性机制应具有三个方面的功能，来防止合法用户在使用数据库时，向数据库注入不合法或不合语义的数据：

(1) 定义功能，提供定义完整性约束条件的机制。

(2) 验证功能，检查用户发出的操作请求是否违背了完整性约束条件。

(3) 处理功能，如果发现用户的操作请求使数据违背了完整性约束条件，则执行相应的动作来保证数据的完整性。

2) 数据库完整性的分类

数据完整性检查是围绕完整性约束条件进行的，因此完整性约束条件是完整性控制机制的核心。

数据库完整性约束分为两种：静态完整性约束和动态完整性约束。完整性约束条件涉及三类作用对象，即属性级、元组级和关系级。这三类对象的状态可以是静态的，也可以是动态的。

静态完整性约束(Static Integrity Constraints)，简称静态约束，是指数据库每一确定状态时的数据对象所应满足的约束条件，它是反映数据库状态合理性的约束，是最重要的一类完整性约束，也称“状态约束”。

动态完整性约束(Dynamic Integrity Constraints)，简称动态约束，不是对数据库状态的约束，而是指数据库从一个正确状态向另一个正确状态的转化过程中新、旧值之间所应满足的约束条件，反映数据库状态变迁的约束，故也称为“变迁约束”。

结合这两种状态，一般将这些约束条件分为静态属性级约束、静态元组级约束、静态关系级约束、动态属性级约束、动态元组级约束、动态关系级约束 6 种约束。

(1) 静态属性级约束。

静态属性级约束是对属性值域的说明，是最常用也是最容易实现的一类完整性约束，包括以下几个方面：

① 对数据类型的约束(包括数据的类型、长度、单位、精度等)。例如，学号必须为字符型，长度为 8。

② 对数据格式的约束。例如，规定学号的前两位表示入学年份，中间两位表示系的编号，后四位表示顺序编号。出生日期的格式为 YY.MM.DD。

③ 对取值范围或取值集合的约束。例如，规定学生的成绩取值范围为 0～100，性别的取值集合为[男，女]，大学本科学生年龄的取值范围为 14～29。

④ 对空值的约束。空值表示未定义或未知的值，它与零值和空格不同。有的属性允许空值，有的不允许取空值。例如学生学号不能取空值，成绩可以为空值。

⑤ 其他约束。例如关于列的排序说明，组合列等。

(2) 静态元组级约束。

一个元组是由若干个列值组成的，静态元组级约束是对元组中各个属性值之间关系的约束。如订货关系中包含订货数量与发货数量这两个属性，其中发货量不得超出订货量；

又如教师关系中包含职称、工资等属性，规定教授的工资不低于1000元。

（3）静态关系级约束。

静态关系级约束是一个关系中各个元组之间，或者若干个关系之间常常存在的各种联系的约束。常见的静态关系级约束有：

① 实体完整性约束。

② 参照完整性约束。

实体完整性约束和参照完整性约束是关系模型的两个极其重要的约束，称为关系的两个不变性。

③ 函数依赖约束。大部分函数依赖约束都在关系模式中定义。

④ 统计依赖约束。统计依赖约束指的是字段值与关系中多个元组的统计值之间的约束关系，如规定总经理的工资不得高于职工的平均工资的4倍，不得低于本部门职工平均工资的3倍，其中，本部门职工的平均工资是一个统计值。

（4）动态属性级约束。

动态属性级约束是修改定义或属性值时应该满足的约束条件。其中包括：

① 修改定义时的约束。例如，将原来允许空值的属性修改为不允许空值时，如果该属性当前已经存在空值，则规定拒绝修改。

② 修改属性值时的约束。修改属性值有时需要参考该属性的原有值，并且新值和原有值之间需要满足某种约束条件。例如，职工工资调整不得低于其原有工资，学生年龄只能增长等。

（5）动态元组级约束。

动态元组级约束是指修改某个元组的值时要参照该元组的原有值，并且新值和原有值间应当满足某种约束条件。例如，职工工资调整不得低于其原有工资＋工龄×1.5等。

（6）动态关系级约束。

动态关系级约束就是加在关系变化前后状态上的限制条件。例如，事务的一致性，原子性等约束。动态关系级约束实现起来开销较大。

6. 数据库完整性的约束

如前所述，要实现由现实系统转换而来的数据库的完整性约束，需先定义约束，并存储于DBMS的约束库中，一旦数据库中的数据要发生变化，则DBMS将根据约束库中的约束，对数据库的完整性进行“验证”。

1）固有约束与隐式约束

（1）固有约束是数据模型所固有的，在DBMS实现时已经考虑，不必额外作说明和定义，只需在数据库设计时遵从这一约束即可。

（2）隐式约束需利用数据库的数据定义语言（DDL）显式定义说明，将约束存储在约束库中，当数据库被更新时，由数据库管理系统进行完整性约束验证。例如，对关系模型来说，利用SQL定义语言，定义相应的实体完整性约束、参照完整性约束、CHECK约束、唯一约束等。

2）显式约束

显式约束的定义方法有过程化定义、断言定义方法、触发器定义方法等。

(1) 过程化定义方法利用过程(或函数)来定义和验证约束。由程序员将约束编写成过程,加入到每个更新数据库的事务中,用以检验数据库更新有否违反规定的约束,如果违反约束条件,则相应的数据更新事务将被异常中止。过程化定义的约束,DBMS 只提供定义途径,不负责约束的验证,过程的定义和验证由程序员在一个过程中由通用程序设计语言编制。这种方法既为程序员编制高效率的完整性验证程序提供了有利的条件,同时也给程序员带来了很大的负担。

(2) 断言定义方法使用一种约束定义语言来定义显式约束,是一种形式化方法。一个断言就是一个谓词,表达了数据库在任何时候都应该满足的一个条件。约束递归语言通常是关系演算语言的变种。显式约束的断言定义方法把约束集合和完整性验证子系统严格分开。约束集合存储在约束库中,完整性验证子系统存取约束库中的约束,将其应用到相应的数据库更新事务中,验证该事务是否违反完整性约束。如发现更新事务违反约束,即退回该事务,否则,允许更新事务的进行。

(3) 触发器定义方法是当特定的事件(如对一个表的插入、删除、修改)发生时,对规则的条件进行检查,如果条件成立,执行规则中的动作,否则不执行该动作。其验证由数据库管理系统负责。

3) 动态约束的定义

动态约束的定义,可以利用 DBMS 为显式约束定义提供的过程化定义方法和触发器定义方法,开发人员通过比较变化前后的数据,决定是否允许数据状态的改变。动态约束的验证过程遵循显式约束的验证过程。

7. 数据库并发控制

1) 并发控制概述

数据库的最大特点之一就是数据资源是共享的,串行执行意味着一个用户在运行程序时,其他用户程序必须等到这个用户程序结束才能对数据库进行存取,这样如果一个用户程序涉及大量数据的输入/输出交换,则数据库系统的大部分时间将处于闲置状态。

因此,为了充分利用数据库资源,很多时候数据库用户都是对数据库系统并行存取数据,这样就会发生多个用户并发存取同一数据块的情况。如果对并发操作不加控制可能会产生不正确的数据,破坏数据的完整性,并发控制就是解决这类问题。并发控制可以保持数据库中数据的一致性,即在任何一个时刻数据库都将以相同的形式给用户提供数据。

2) 事务

并发控制是以事务(transaction)为单位进行的。事务是数据库的逻辑工作单位,它是用户定义的一组操作序列。但并不是任意的数据操作序列都能成为事务,为了保护数据的完整性,事务要求处理时必须满足 ACID 原则,即事务必须具有以下特征:

(1) 原子性。

原子性(Atomic)是指一个事务是一个不可分割的工作单位,事务在执行时,应该遵守"要么不做,要么全做"的原则,即不允许事务部分的完成。

(2) 一致性。

一致性(Consistency)是指事务执行的结果必须是使数据库从一个一致性状态变到另一个一致性状态。例如前面的转账如果只执行其中一个操作,则数据库处于不一致状态,账

务会出现问题。也就是说，两个操作要么全做，要么全不做，否则就不能成为事务。

(3) 隔离性。

隔离性(Isolation)是指数据库中一个事务的执行不能被其他事务干扰。即一个事务内部的操作及使用的数据对并发的其他事务是隔离的。并发控制就是为了保证事务间的隔离性。

(4) 持久性(Durability)。

持久性(Durability)指一个事务一旦提交，它对数据库中数据的改变就应该是持久的，即使数据库因故障而受到破坏，DBMS也应该能够恢复。

(5) 正确调度。

保证事务ACID特性是事务处理的重要任务，而事务ACID特性可能遭到破坏的原因之一是多个事务对数据库的并发操作造成的。为了保证事务的隔离性和保证数据库的一致性，DBMS需要对并发操作进行正确调度。这些就是数据库管理系统中并发控制机制的责任。

3) 并发操作导致的不一致性

一般地说，并发操作带来的数据不一致性主要包括以下三类：

(1) 丢失修改。

事务1与事务2从数据库中读入同一数据并修改，事务2的提交结果破坏了事务1提交的结果，导致事务1的修改被丢失。

(2) 不可重复读。

事务1读取数据后，事务2执行更新操作，使事务1无法再现前一次读取结果。

(3) 读“脏”数据。

事务1修改某一数据，并将其写回磁盘，事务2读取该修改后的数据后，事务1由于某种原因被撤销，这时事务1已修改过的数据恢复原值，事务2读到的数据就与数据库中的数据不一致，是不正确的数据，又称为“脏”数据。

产生上述三类数据不一致性的主要原因是并发操作破坏了事务的隔离性。并发控制就是要用正确的方式调度并发操作，使一个用户事务的执行不受其他事务的干扰，从而避免造成数据的不一致性。

另一方面，对数据库的应用有时允许某些不一致性，例如有些统计工作涉及数据量很大，读到一些“脏”数据对统计精度没什么影响，这时可以降低对一致性的要求以减少系统开销。

并发控制的主要方式是封锁机制，即加锁(Locking)。

4) 加锁

加锁就是事务T在对某个数据操作之前，先向系统发出请求，对其加锁。加锁后事务T对其要操作的数据具有了一定的控制权，在事务T释放它的锁之前，其他事务不能操作这些数据。

确切的控制由封锁的类型决定。基本的封锁类型有两种：排他锁(Exclusive Locks，X锁)和共享锁(Share Locks，S锁)。

排他锁又称为写锁。若事务T对数据对象A加上X锁，则只允许事务T读取和修改A，其他事务任何事务都不能再对A加任何类型的锁，直到事务T释放A上的锁。这就保证了其他事务在事务T释放A上的锁之前不能再读取和修改A。

共享锁又称为读锁。若事务 T 对数据对象 A 加上 S 锁，则事务 T 可以读 A 但不能修改 A，其他事务只能再对 A 加 S 锁，而不能加 X 锁，直到事务 T 释放 A 上的 S 锁。这就保证了其他事务可以读 A，但在事务 T 释放 A 上的 S 锁之前不能对 A 做任何修改。

5）封锁协议

封锁可以保证合理地进行并发控制，保证数据的一致性。在封锁时，要考虑一定的封锁规则，例如，何时开始封锁、封锁多长时间、何时释放等，这些封锁规则称为封锁协议。对封锁方式规定不同的规则，就形成了各种不同的封锁协议。封锁协议在不同程度上对正确控制并发操作提供了一定的保证。并发操作所带来的丢失修改、污读和不可重读等数据不一致性问题，可以通过三级封锁协议在不同程度上给予解决。

（1）一级封锁协议。

一级封锁协议是事务 T 在修改数据 R 之前必须先对其加 X 锁，直到事务结束才释放。事务结束包括正常结束（COMMIT）和非正常结束（ROLLBACK）。

一级封锁协议可防止丢失修改，并保证事务 T 是可恢复的。

在一级封锁协议中，如果仅仅是读数据不对其进行修改，是不需要加锁的，所以它不能保证可重复读和不读“脏”数据。

（2）二级封锁协议。

二级封锁协议是一级封锁协议加上事务 T 在读取数据 R 之前必须先对其加 S 锁，读完后即可释放 S 锁。

在二级封锁协议中，除了可以防止丢失修改，还可以进一步防止读“脏”数据。由于读完数据后即可释放 S 锁，所以它不能保证可重复读。

（3）三级封锁协议。

三级封锁协议是一级封锁协议加上事务 T 在读取数据 R 之前必须先对其加 S 锁，直到事务结束才释放。三级封锁协议除了防止丢失修改和不读“脏”数据外，还进一步防止了不可重复读。

上述三级协议的主要区别在于什么操作需要申请封锁，以及何时释放锁（即持锁时间）。

6）活锁和死锁

封锁的方法和操作系统一样可能引起活锁和死锁。

（1）活锁。

如果事务 T1 封锁了数据 R，事务 T2 又请求封锁数据 R，于是事务 T2 等待。事务 T3 也请求封锁数据 R，当事务 T1 释放了数据 R 上的封锁之后系统首先批准了事务 T3 的请求，事务 T2 仍然等待。然后事务 T4 又请求封锁 R，当事务 T3 释放了数据 R 上的封锁之后系统又批准了事务 T4 的请求……事务 T2 有可能永远等待，这就是活锁的情形，避免活锁的简单方法是采用先来先服务的策略。当多个事务请求封锁同一数据对象时，封锁子系统按请求封锁的先后次序对事务排队，数据对象上的锁一旦释放就批准申请队列中第一个事务获得锁。

（2）死锁。

封锁技术可有效解决并行操作的一致性问题，但也可产生新的问题，即死锁问题。在同时处于等待状态的两个或多个事务中，其中的每一个在它能够进行之前，都等待着某个数据，而这个数据已被它们中的某个事务所封锁，这种状态称为死锁。

7）预防死锁的方法

死锁一旦发生，系统效率将会大大下降，因而要尽量避免死锁的发生。预防死锁的方法有多种，常用的方法有以下两种：

（1）一次封锁法。

每个事务一次将所有要使用的数据全部依次加锁，并要求加锁成功，只要一个加锁不成功，表示本次加锁失败，则应该立即释放所有已加锁成功的数据对象，然后重新开始从头加锁。

（2）顺序封锁法。

顺序封锁法是预先对所有可加锁的数据对象规定一个加锁顺序，每个事务都需要按此顺序加锁，在释放时，按逆序进行。

在操作系统中广为采用的预防死锁的策略并不适合数据库的特点，因此DBMS在解决死锁的问题上普遍采用的是诊断并解除死锁的方法。

数据库系统中诊断死锁的方法与操作系统类似，一般使用超时法或事务等待图法。

① 超时法：如果一个事务的等待时间超过了规定的时限，就认为发生了死锁。超时法实现简单，但其不足也很明显。一是有可能误判死锁，事务因为其他原因使等待时间超过时限，系统会误认为发生了死锁。二是时限若设置得太长，死锁发生后不能及时发现。

② 事务等待图法：事务等待图是一个有向图G=(T,U)。T为结点的集合，每个结点表示正运行的事务；U为边的集合，每条边表示事务等待的情况。若T1等待T2，则T1，T2之间划一条有向边，从T1指向T2。事务等待图动态地反映了所有事务的等待情况。并发控制子系统周期性地(比如每隔1 min)检测事务等待图，如果发现图中存在回路，则表示系统中出现了死锁。

DBMS的并发控制子系统一旦检测到系统中存在死锁，就要设法解除。通常采用的方法是选择一个处理死锁代价最小的事务，将其撤销，释放此事务持有的所有的锁，使其他事务得以继续运行下去。当然，对撤销的事务所执行的数据修改操作必须加以恢复。

8．数据库的恢复

虽然数据库系统中已采取一定的措施，来防止数据库的安全性和完整性的破坏，保证并发事务的正确执行，但数据库中的数据仍然无法保证绝对不遭受破坏，比如计算机系统中硬件的故障、软件的错误、操作员的失误，恶意的破坏等都有可能发生，这些故障的发生影响数据库数据的正确性，甚至可能破坏数据库，使数据库中的数据全部或部分丢失。

系统必须具有检测故障并把数据库从错误状态中恢复到某一正确状态的功能，这就是数据库的恢复。

1）数据恢复策略

数据库运行过程中可能会出现各种各样的故障，这些故障可分为以下三类：事务故障、系统故障和介质故障。根据故障类型的不同，应该采取不同的恢复策略。

（1）事务故障的恢复。

事务故障是指事务在运行到正常结束前被终止，这时恢复子系统可以利用日志文件撤销此事务对数据库已进行的修改。

日志文件是用来记录事务对数据库的更新操作的文件。日志文件内容包括事务标识

(标明是哪个事务)、操作类型(插、删或改)、操作前后的数据值等。目的是为数据库的恢复保留详细的数据。

恢复的过程为:反向扫描日志文件并执行相应操作的逆操作事务故障的恢复是由系统自动完成的,对用户是透明的。

(2) 系统故障的恢复。

系统故障是指系统在运行过程中,由于某种原因,造成系统停止运转,致使所有正在运行的事务都以非正常方式终止,要求系统重新启动。

引起系统故障的原因可能有:硬件错误(如 CPU 故障)、操作系统或 DBMS 代码错误、突然断电等。

系统故障的恢复是系统在重启时自动完成的,不须用户干预。

恢复过程为:正向扫描日志文件,找出故障发生前已提交的事务,将其重做;同时找出故障发生时未完成的事务,并撤销这些事务。

(3) 介质故障的恢复。

介质故障是指系统在运行过程中,由于辅助存储器介质受到破坏,使存储在外存中的数据部分丢失或全部丢失。

介质故障发生后,磁盘上的物理数据和日志文件均遭到破坏,恢复的方法是首先重装数据库,使数据库管理系统能正常运行,然后利用介质损坏前对数据库已做的备份或利用镜像设备恢复数据库。

2) 数据恢复的方法

(1) 数据转储。

将整个数据库进行转储,把它复制到备份介质中保存起来,这些备用的数据库文件称为后备副本,以备恢复之用。

转储通常可以分为静态转储和动态转储。静态转储在系统中无运行事务时进行转储操作,转储开始时数据库处于一致性状态,转储期间不允许对数据库的任何存取、修改活动。动态转储在转储期间允许对数据库进行存取或修改,转储操作与用户事务并发进行。动态转储不能保证副本中的数据正确有效。需要把动态转储期间各事务对数据库的修改活动登记下来,建立日志文件,后备副本加上日志文件才能把数据库恢复到某一时刻的正确状态。

(2) 利用事务日志。

利用事务日志可以恢复非完整事务。从非完整事务当前值按事务日志记录的顺序反向执行(Undo),直到数据库恢复到事务开始时的状态为止。

6.3.4 数据容灾

1. 数据容灾概述

1) 数据容灾的概念

数据容灾(Disaster Tolerance),就是在灾难发生时,在保证应用系统的数据尽量少丢失的情况下,维持系统业务的连续运行。

与数据容灾比较容易混淆的概念有容错和灾难恢复。容错是指在计算机系统软硬件发生故障时,保证系统能继续运行的能力,主要通过硬件冗余和错误检查等技术来实现;容灾

是通过系统冗余、灾难检测和系统迁移等技术来实现。灾难恢复是指灾难发生后，系统恢复正常运行的能力；而容灾指灾难发生时保持系统不间断运行的能力。

2）数据容灾的分类

由于容灾包含的内容比较广泛，对容灾的分类也可以从多个方面进行。总的来讲，可以从容灾的范围、容灾的技术和对灾难的防御程度来区分。

从容灾的范围讲，容灾分成本地容灾、近距离容灾和远距离容灾。这三种容灾能容忍的灾难是不相同的，采用的容灾技术也是不同的。

目前有很多种容灾技术，种类也比较复杂。但总体上可以区分为离线式容灾（冷容灾）和在线式容灾（热容灾）两种类型。

① 离线式容灾主要依靠备份技术来实现。首先通过备份软件将数据备份到磁带上，然后将磁带异地保存、管理。数据的备份过程可以实现自动化管理，整个方案的部署和管理比较简单，投资较少。缺点在于：系统的数据恢复较慢，备份窗口内的数据丢失严重，实时性差。对 RTO（Recovery Time Objective）和 RPO（Recovery Point Objective）要求较低的用户可以选择这种方式。

② 在线式容灾中，源数据中心和容灾中心同时工作。数据在写入源数据中心的同时，实时地被复制传送到容灾中心。在此基础上，可以在应用层进行集群管理，当业务中心遭受灾难、出现故障时，可由容灾中心自动接管并继续提供服务。应用层的管理一般由专门的软件来实现，可以代替管理员实现自动管理。在线容灾可以实现数据的实时复制，因此，数据恢复的 RTO 和 RPO 都可以满足用户的高要求。因此，数据重要性很高的用户都应选择这种方式，比如金融行业的用户等。实现这种方式的容灾需要很高的投入。

容灾备份系统按照灾难防御程度的不同，可分为数据容灾和应用容灾。

数据容灾是对应用系统数据按照一定的策略进行异地容灾备份，当灾难发生时，应用系统暂时无法正常运行，必须花费一定时间从灾备中心恢复应用关键数据至本地系统以保证业务的连续性和数据的完整性，因为异地容灾备份系统只保存了灾难发生前应用系统的备份数据，因此数据容灾可能会产生部分数据丢失。

应用容灾是在异地建立一个与本地应用系统相同的备份应用系统，两个系统同步运行，当灾难发生时，异地系统会迅速接管本地系统继续业务的运行，不需要中断业务，这样使得应用系统使用者察觉不到灾难的发生。应用容灾比数据容灾防御灾难破坏能力要强，它能够更好地保持业务的连续性和数据的完整性，而数据容灾会出现业务的暂时中断，需要花费一定的时间后才能重新维持业务的连续性，并且可能产生部分数据的丢失。

3）容灾等级的划分

数据容灾备份是通过在异地建立和维护一个存储备份系统，利用地理上的分离来保证系统和数据对灾难性事件的抵御能力。

根据对灾难的容忍能力、系统恢复所用的时间及数据丢失的程度，数据容灾备份系统可以分为七个等级。

第 0 级：本地数据容灾。即只能在本地进行数据备份，数据本地保存。当灾难发生时，只有很低的灾难恢复能力，而且无法保证业务的连续性。

第 1 级：本地应用容灾。当因磁盘损坏等灾难发生时，系统能够迅速切换，保证业务的连续性。

第 2 级：异地数据冷备份。将本地关键数据进行备份，并送往异地保存。当灾难发生时，对系统关键数据进行恢复。该级别的数据备份成本低，但存储介质难管理，当灾难出现时，损失的数据量大。

第 3 级：异地异步数据容灾。在异地建立一个数据备份站点，通过网络采用异步方式进行数据备份。当灾难发生时，利用备份站点的数据进行恢复。它与第 2 级别的灾难容忍程度相同，但它采用网络进行数据复制，两站点数据同步程度高。

第 4 级：异地同步数据容灾。在异地建立一个数据备份站点，通过网络以同步方式进行数据备份。当灾难发生时，数据丢失量比第 3 级小，但与第 3 级存在同样的问题，就是数据恢复速度慢，无法保证业务连续性。

第 5 级：异地异步应用容灾。在异地建立一个与源应用系统完全相同的备用系统，并采用异步的方式进行数据同步。当灾难发生时，备用系统接替源问题系统继续工作，但会存在少了数据丢失。

第 6 级：异地同步应用容灾。在异地建立一个与源应用系统完全相同的备用系统，并采用同步方式进行数据复制。当灾难发生时，备用系统完全接替源问题系统进行工作，并且可以实现数据零丢失。

4）容灾系统的指标

从技术上看，衡量容灾系统有三个主要指标：RPO、RTO 和备份窗口（backup window）。

（1）RPO（Recovery Point Objective），即数据恢复点目标。

（2）RTO（Recovery Time Objective），即恢复时间目标。

（3）备份窗口（backup window），一个备份窗口指的是在不严重影响使用待备份数据的应用程序的情况下，完成一次给定备份的时间间隔，由需要备份数据的总量和处理数据的服务架构的速度来决定。为了保证备份数据的一致性，在备份过程中数据不能被更改，所以在某些情况下，备份窗口是数据和应用不可用的间隔时间。

5）容灾系统评审标准

目前，国际上通用的容灾系统的评审标准为 Share78，其主要内容如下：

（1）备份/恢复的范围；

（2）灾难恢复计划的状态；

（3）业务中心与容灾中心之间的距离；

（4）业务中心与容灾中心之间如何相互连接；

（5）数据是怎样在两个中心之间传送的；

（6）允许有多少数据被丢失；

（7）怎样保证更新的数据在容灾中心被更新；

（8）容灾中心可以开始容灾进程的能力。

Share78 只是建立容灾系统的一种评审标准，在设计容灾系统时，还需要提供更加具体的设计指标。建立容灾系统的最终目的，是为了在灾难发生后能够以最快的速度恢复数据服务，所以，容灾中心的设计指标主要与容灾系统的数据恢复能力有关。

2. 数据容灾技术

传统的容灾技术通常指针对数据业务系统的灾难采用的远程备份系统技术。随着对容灾系统要求的不断提高，容灾技术也不断进步。

一般地说，在容灾系统中，实现数据容灾和应用容灾可以采取不同的实现技术。数据容灾的技术主要包括数据备份技术、数据复制技术等，而应用容灾技术则主要包括灾难检测技术、系统迁移技术等。

1) 数据备份技术

数据备份就是把数据从业务系统备份到备份系统介质中的过程。数据备份技术最初是备份到本地磁带，随着网络技术的发展，备份技术也有了飞速的进步。

(1) 主机备份。

这种备份就是传统意义上的基于主机(Host-based)的备份。主机负责将数据备份到和主机直接相连的存储介质上(一般是磁带)。虽然这种备份的速度快，管理简单，但是仅能适应于单台服务器备份，并且在灾难恢复过程中，系统恢复的时间长。

(2) 网络备份。

随着网络的发展，传统的主机备份渐渐地转向了网络备份，即系统中备份数据的传输以网络为基础。根据备份系统中备份服务器、介质服务器是否在同一个 LAN 中，可以将网络备份分为基于局域网的备份和远程网络备份。

① 基于局域网的备份特点是应用服务器、备份服务器和介质服务器共用一个局域网络，备份服务器统一管理备份的过程，多个应用服务器可以将各自的数据备份到介质服务器上。这种备份方式可以共享介质资源，实现集中的备份管理。缺点是对网络带宽和备份时间的压力比较大，并且不具备远程的容灾能力。当然通过将介质(磁盘、磁带或光盘)运输到远程保存，可以具备一定的容灾能力。

② 远程网络备份，则是介质服务器与应用服务器不属于同一个局域网，备份服务器依然统一管理备份的过程，备份数据则是通过 WAN、ATM 或者 Internet 等公共网络传送到远程的介质服务器上。这种备份方式基本上构成了一个异地的备份容灾方案。由于备份数据在公共网络上传输，备份的速度、备份数据的完整性和安全性等方面都需要考虑。

(3) 专有存储网络备份。

当存储系统成为一个独立于备份系统的系统之后，特别是存储局域网(Storage Area Network，SAN)的发展，使得备份过程可以在存储局域网中实现，根据备份过程中对应用服务器的影响，专有存储网络备份可以分为 LAN-Free 备份和 Server-Free 备份。

① LAN-Free 备份，是在存储网络(Storage Network)之上建立的一种备份系统。在该备份系统中，业务系统的存储和介质服务器的存储直接通过专用存储网络进行连接，在备份过程中，庞大的备份数据不经过主机系统所在的网络，而是通过专用的存储网络传输到介质上。这种备份方式的优点是共享介质资源，实现集中管理，不会对主机系统网络有影响。缺点是实现比较复杂，成本相对较高。

② Server-Free 备份，则是建立在存储局域网(Storage Area Network，SAN)的基础上，备份过程无须应用服务器参与数据传输的备份系统。这种备份方式可以保证业务系统及其网络不受影响。目前这种备份技术还不太成熟，对硬件的性能和兼容性的要求都很高。

专用存储网络备份更多关注的是存储系统的扩展性、可用性以及性能等方面的因素，因此存储局域网的发展将会在更大程度上提高系统的数据容灾能力。

2）数据复制技术

和数据备份相比，数据复制技术则是通过不断将业务系统的数据复制到另外一个不同的备份系统中，以保证在灾难发生时，业务系统的数据丢失量最少。

按照备份系统中数据是否与业务系统同步，数据复制可以分成同步数据复制和异步数据复制。同步数据复制就是将本地业务系统的数据以完全同步的方式复制到备份系统中。由于发生在业务系统的每一次I/O操作都需要等待远程复制完成才能返回，这种复制方式虽然可能做得数据的零丢失，但是对系统的性能有很大的影响。异步数据复制则是将本地业务系统中的数据在后台异步地复制到备份系统中。这种复制方式会有少量的数据丢失，但是对业务系统的性能影响较小。根据数据复制的层次，数据复制技术的实现可以分成以下四种：

（1）存储系统数据复制。

数据的复制过程通过本地的存储系统和远端的存储系统之间的通信完成。这种方式的复制对应用来讲是透明的，可以直接实现数据容灾功能，也可以提供很高的性能，可是，对存储系统的要求比较高。

（2）交换层数据复制。

这种方式的复制技术是伴随着存储局域网的出现引入的，即在存储局域网的交换层上实现数据复制。实现方式可以通过专有的复制服务器实现，也可以通过存储局域网（SAN）交换机，将数据同步地复制到远端存储系统中。

（3）操作系统层数据复制。

这种方式主要通过操作系统或者数据卷管理器来实现对数据的远程复制。这种复制技术往往要求本地系统和远端系统是同构的，并且由于数据复制由主机系统完成，其效率和管理上也存在不少问题。

（4）应用程序层数据复制。

例如数据库的异地复制技术，通常采用日志复制功能，依靠本地和远程主机间的日志归档与传递来实现两端的数据一致。这种复制技术对系统的依赖性小，有很好的兼容性。缺点是本地应用程序向远端复制的是日志文件，这需要远端应用程序重新执行和应用才能产生可用的备份数据。另外，由于各个应用程序采取的复制技术不同，无法以一种技术实现多种应用的数据复制。

3）灾难检测技术

对于一个容灾系统来讲，在灾难发生时，尽早地发现业务系统端的灾难，尽快地恢复业务系统的正常运行或者尽快地将业务迁移到备用系统上，都可以将灾难造成的损失降低到最低。除了依靠人力来对灾难进行确定之外，对于系统意外停机等灾难还需要容灾系统能够自动地检测灾难的发生，目前容灾系统的检测技术一般采用心跳技术。

心跳技术的实现方法是：业务系统在空闲时每隔一段时间向外广播一下自身的状态。检测系统在收到这些“心跳信号”之后，便认为业务系统是正常的，否则，在给定的一段时间内没有收到“心跳信号”，检测系统便认为业务系统出现了非正常的灾难。心跳技术的另外一个实现是：每隔一段时间，检测系统就对业务系统进行一次检测，如果在给定的时间内，被检测的系统没有响应，则认为被检测的系统出现了非正常的灾难。心跳技术中的关键点

是心跳检测的时间和时间间隔周期。如果间隔周期短，会对系统带来很大的开销。如果间隔周期长，则无法及时地发现故障。

4）系统迁移技术

灾难发生后，为了保持业务系统的业务连续性，需要实现系统的透明性迁移，利用备用系统透明地代替业务系统进行运作。一般对实时性要求不高的容灾系统，例如 Web 服务、邮件服务器等，可以通过修改 DNS 或者 IP 来实现；对实时性要求高的容灾系统，则需要将业务系统的应用透明地迁移到备用系统上。目前基于本地机群的进程迁移的算法可以应用在远程容灾系统中，但是需要对迁移算法进行改进，使之适应复杂的网络环境。

上述几种技术只是应用在容灾系统中最广泛的技术。随着技术的更新发展，现在有许多的技术都已经开始应用于容灾系统，例如存储技术中的 SAN、NAS、虚拟化技术和快照技术、持续数据保护（CDP）等等；数据管理中的数据归档、迁移和内容存储等技术；还有基于冗余技术和机群技术的高可用技术等等。这些技术的引入必将对容灾系统产生深远的影响。

3. 容灾方案的应用方案

目前比较完善的容灾系统的设计，一般都为三级体系结构的容灾系统，整个系统包括存储子系统、备份子系统和灾难恢复子系统三大部分。

下面以惠普公司生产的备份服务器、模块化磁盘阵列、备份磁带库和相关容灾软件为例，介绍基于三级体系结构建立容灾系统的方案。

1）数据存储子系统

在正常情况下，业务系统运行在主中心服务器上，业务数据存储在主中心存储磁盘阵列 EMA12000 中。EMA12000 具有从 12 个磁盘驱动器到最多 126 个磁盘驱动器的扩展能力，能跨越多个大型主机和混合的 UNIX、多厂商的 Windows NT、Windows 2000 以及其他开放系统的平台。

惠普为 EMA12000 系统设计的 ASC 阵列控制软件，实现了对跨多服务器平台数据的集中式控制，使数据不管在何时、何地以及何种方式需要，其可用性都能以真正的零停机时间得到成分保证。

2）数据备份子系统

为了实现业务数据的实时灾难备份功能，关键应用可设置两个数据中心，分别是主中心和备份中心。主中心系统配置主机包括两台或多台 HP ALPHA 服务器以及其他相关服务器，通过构成 SCSI CLUSTER 组成多机高可靠性环境。主中心通过 ATM/E3/WDM 与备份中心连接。

在容灾系统解决方案中，正常情况下，业务系统运行在主中心服务器上，业务数据存储在主中心存储磁盘阵列 EMA12000 中，同时在备份中心配置 EMA12000 存储磁盘阵列。主中心存储磁盘阵列通过 ATM/E3/WDM 连接到备份中心磁盘阵列，DRM（数据复制管理器）使主中心存储数据与备份中心数据保持实时完全一致。

3）灾难恢复子系统

方案中，备份数据的磁带库安置在备份中心，利用备份服务器直接连接到存储阵列 EMA12000 和磁带库 TL895，通过 EBS（企业数据备份）和 Legato NetWorker 数据存储管

理系统控制系统的备份。万一主数据中心出现意外灾难,系统可以自动切换到备份数据中心,在保持连续运行的基础上,快速恢复主数据中心的业务数据。

该套三级体系容灾方案具有高度的可用性。第一级,为了避免系统单点失败而影响整个系统的情况出现,采用了冗余的手段,大到主机,存储设备,小到光纤适配器,均具备冗余容错功能;第二级,无论是主机或存储设备出现故障,均可通过主/备份中心光纤交换机之间的连接来保证通信和数据的完整性;第三级,万一主数据中心出现意外灾难,系统可以自动切换到备份数据中心。三级体系的科学设计保证了数据容灾系统的高度可用性和可靠性。

不仅如此,惠普独有的 HP OpenView 网络设备管理软件从根本上将系统管理人员解脱出来。整个系统的设备虽然很多,但不论是主机系统、存储设备,还是光纤交换机、光纤卡,均能通过一台工作站进行集中的管理和监控,从另一个方面保证了整个业务系统的连续不断地运行。除正常的计划性停机外,该系统可以做到 365×24 的可用性。

6.4 数据隐私保护

6.4.1 隐私保护概述

1. 隐私的定义

简单地说,隐私就是个人、机构等实体不愿意被外部世界知晓的信息。在具体应用中,隐私即为数据所有者不愿意被披露的敏感信息,包括敏感数据以及数据所表征的特性。通常我们所说的隐私都指敏感数据,如个人的亲属、薪资、病人的患病记录、公司的财务信息等。但当针对不同的数据以及数据所有者时,隐私的定义也会存在差别的。保守的病人会视某种疾病(例如患癌症)信息为隐私,而开放的病人却不视之为隐私。

一般来说,从隐私所有者的角度而言,隐私可以分为两类,即个人隐私、共同隐私;从隐私的具体内容来分类,隐私又可以分为三类,即数据隐私、位置隐私、轨迹隐私。

1) 个人隐私

个人隐私(Individual privacy)是指任何可以确认特定个人或与可确认的个人相关、但个人不愿被暴露的信息,都叫做个人隐私,如身份证号、医疗记录等。

2) 共同隐私

共同隐私(Corporate privacy)不仅包含个人的隐私,还包含所有个人共同表现出来但不愿被暴露的信息。如公司员工的平均薪资、薪资分布等信息。

2. 隐私的度量

数据隐私保护的效果,是由通过攻击者披露隐私的多少来侧面反映的。现有的隐私度量都可以统一用“披露风险”(Disclosure Risk)来描述。披露风险表示攻击者根据所发布的数据和其他背景知识(Background Knowledge),可能披露隐私的概率。通常,关于隐私数据的背景知识越多,披露风险越大。

若 s 表示敏感数据,事件 S_k 表示“攻击者在背景知识 K 的帮助下揭露敏感数据 s”,则披

露风险 $r(s,K)$ 表示为：

$$r(s,K)=\Pr(S_k)$$

对数据集而言，若数据所有者最终发布数据集 D 的所有敏感数据的披露风险都小于阈值 α，$\alpha\in[0,1]$，则称该数据集的披露风险为 α。例如，静态数据发布原则 *l-diversity* 保证发布数据集的披露风险小于 $1/l$，动态数据发布原则 *m-Invariance* 保证发布数据集的披露风险小于 $1/m$。

特别地，不做任何处理所发布数据集的披露风险为 1；当所发布数据集的披露风险为 0 时，这样发布的数据被称为实现了完美隐私(Perfect Privacy)。完美隐私实现了对隐私最大程度的保护，但由于对攻击者先验知识的假设本身是不确定的，因此实现对隐私的完美保护也只在具体假设、特定场景下成立，真正的完美保护并不存在。

3. 数据隐私保护技术的分类

没有任何一种隐私保护技术能够适用于所有的应用。本书将数据隐私保护技术分为三类：

1）基于数据失真(Distorting)的技术

基于数据失真的技术是使敏感数据失真但同时保持某些数据或数据属性不变的方法。例如，采用添加噪声(Adding Noise)、交换(Swapping)等技术对原始数据进行扰动处理，但要求保证处理后的数据仍然可以保持某些统计方面的性质，以便进行数据挖掘等操作。

2）基于数据加密的技术

基于数据加密的技术是采用加密技术在数据挖掘过程中隐藏敏感数据的方法。多用于分布式应用环境中，如安全多方计算(Secure Multiparty Computation，SMC)。

3）基于限制发布的技术

基于限制发布的技术是根据具体情况有条件地发布数据。如：不发布数据的某些域值，数据泛化(Generalization)等。

此外，许多隐私保护的新技术，由于其融合了多种技术，很难将其简单地归到以上某一类，但它们在利用某类技术的优势的同时，将不可避免的引入其他的缺陷。基于数据失真的技术，效率比较高，但却存在一定程度的信息丢失；基于加密的技术则刚好相反，它能保证最终数据的准确性和安全性，但计算开销比较大；而限制发布技术的优点是能保证所发布的数据一定真实，但发布的数据会有一定的信息丢失。

4. 隐私保护技术的性能评估

隐私保护技术需要在保护隐私的同时，兼顾对应用的价值以及计算开销。通常从以下三方面对隐私保护技术进行度量：

1）隐私保护度

隐私保护度通常通过发布数据的披露风险来反映，披露风险越小，隐私保护度越高。

2）数据缺损

数据缺损是对发布数据质量的度量。它反映通过隐私保护技术处理后数据的信息丢失，数据缺损越高，信息丢失越多，数据利用率(Utility)越低。具体的度量有信息缺损(Information Loss)、重构数据与原始数据的相似度等。

3）算法性能

算法性能一般利用时间复杂度对算法性能进行度量。例如，采用抑制（Suppression）实现最小化的 k-匿名问题已经证明是 NP-hard 问题；时间复杂度为 $O(k)$ 的近似 k-匿名算法，显然优于复杂度为 $O(k\log k)$ 的近似算法。均摊代价（Amortized Cost）是一种类似于时间复杂度的度量，它表示算法在一段时间内平均每次操作所花费的时间代价。除此之外，在分布式环境中，通信开销（Communication Cost）也常常关系到算法性能，常作为衡量分布式算法性能的一个重要指标。

6.4.2 基于数据失真的隐私保护技术

数据失真技术通过扰动（Perturbation）原始数据来实现隐私保护。它要使扰动后的数据同时满足：

（1）攻击者不能发现真实的原始数据。也就是说，攻击者通过发布的失真数据不能重构出真实的原始数据。

（2）失真后的数据仍然保持某些性质不变，即利用失真数据得出的某些信息等同于从原始数据上得出的信息。这就保证了基于失真数据的某些应用的可行性。

当前，基于数据失真的隐私保护技术包括随机化、阻塞（Blocking）、交换、凝聚（Condensation）等。一般地，当进行分类器构建和关联规则挖掘，而数据所有者又不希望发布真实数据时，可以预先对原始数据进行扰动后再发布。

1. 随机化

数据随机化即是对原始数据加入随机噪声，然后发布扰动后数据的方法。需要注意的是，随意对数据进行随机化并不能保证数据和隐私的安全，因为利用概率模型进行分析常常能披露随机化过程的众多性质。随机化技术包括两类：随机扰动（Random Perturbation）和随机化应答（Randomized Response）。

1）随机扰动

随机扰动采用随机化过程来修改敏感数据，从而实现对数据隐私的保护。

对外界而言，只可见扰动后的数据，从而实现了对真实数据值的隐藏。但扰动后数据仍然保留着原始数据分布 X 的信息，通过对扰动后的数据进行重构，可以恢复原始数据分布 X 的信息。但不能重构原始数据的精确值 x1，x2，…，xn。

随机扰动技术可以在不暴露原始数据的情况下进行多种数据挖掘操作。由于通过扰动数据重构后的数据分布几乎等同于原始数据的分布，因此利用重构数据的分布进行决策树分类器训练后，得到的决策树能很好地对数据进行分类。在关联规则挖掘中，通过往原始数据注入大量伪项（False Item）来对频繁项集进行隐藏，再通过在随机扰动后的数据上估计项集支持度，从而发现关联规则。除此之外，随机扰动技术还可以应用到 OLAP 上实现对隐私的保护。

2）随机化应答

随机化应答的基本思想是：数据所有者对原始数据扰动后发布，使攻击者不能以高于预定阈值的概率得出原始数据是否包含某些真实信息或伪信息。虽然发布的数据不再真实，但在数据量比较大的情况下，统计信息和汇聚（Aggregate）信息仍然可以较为精确地被

估算出。随机化应答技术与随机扰动技术的不同之处在于敏感数据是通过一种应答特定问题的方式间接提供给外界的。

随机化应答模型有两种：相关问题模型(Related-Question Model)和非相关问题模型(Unrelated-Question Model)。相关问题模型是通过设计两个关于敏感数据的对立问题，如：我含有敏感值 A 我没有敏感值 A。

数据所有者根据自己拥有的数据随机选取一个问题进行应答，但不让提问者知道回答的具体问题。当大量数据所有者进行回答后，通过计算可以得出含有敏感值的应答者比例和不含敏感值应答者的比例。假设应答者随机选取含有敏感值 A 的概率为 θ，则以下等式成立：

$$P*(A=yes)=P(A=yes)\cdot\theta+P(A=no)\cdot(1-\theta)$$

$$P*(A=no)=P(A=no)\cdot\theta+P(A=yes)\cdot(1-\theta)$$

其中 P*(A=yes)是回答中 yes 的比例，P(A=yes)是含有敏感值 A 的数据所有者的比例。通过以上两个等式，联合对所有应答进行估计得出的 P*(A=yes)和 P*(A=no)，可以得到含有(或不含有)敏感值 A 的数据所有者比例 P(A=yes)(或 P(A=no))。

在这整个过程中，由于不能确定与应答者回答的相关问题，因此不能确定其是否含有敏感数据值。由于基于随机化应答技术采用应答模式提供信息，因此多用于处理分类数据(Categorical Data)。

MASK(Mining Associations with Secrecy Konstraints)是一种基于随机化应答技术的布尔关联规则挖掘算法。它利用预先定义的分布函数产生随机数并对原始数据进行扰动，数据使用者基于扰动数据，结合应答信息对数据进行重构，在此基础上，估计出项集的支持度从而找出频繁项集。

2. 凝聚技术

随机化技术一个不可避免的缺点是：针对不同的应用都需要设计特定的算法对转换后的数据进行处理，因为所有的应用都需要重建数据的分布。针对这一缺点，研究者提出了凝聚技术，即将原始数据记录分成组，每一组内存储由 k 条记录产生的统计信息，包括每个属性的均值、协方差等。这样，只要是采用凝聚技术处理的数据，都可以用通用的重构算法进行处理，并且重构后的记录并不会披露原始记录的隐私，因为同一组内的 k 条记录是两两不可区分的。

3. 阻塞技术

与随机化技术修改数据、提供非真实数据的方法不同，阻塞技术采用的是不发布某些特定数据的方法，因为某些应用更希望基于真实数据进行研究。阻塞技术具体反应到数据表中，即是将某些特定的值用一个不确定符号代替。例如，通过引入除{0,1}外的代表不确定值的符号“?”可以实现对布尔关联规则的隐藏。由于某些值被“?”代替，那么对某些数据项集的计数则为一个不确定的值，位于一个最小估计值和最大估计值范围内。因此，对于敏感关联规则的隐藏即是设计一种算法，在阻塞尽量少的数据值情况下，将敏感关联规则可能的支持度和置信度控制在预定的阈值以下。类似于对关联规则的隐藏，利用阻塞技术还可以实现对分类规则的隐藏。

6.4.3 基于数据加密的隐私保护技术

在分布式环境下实现隐私保护，要解决的重要问题是通信的安全性，而加密技术正好满足这个需求。因此，基于数据加密的隐私保护技术多用于分布式应用中，如分布式数据挖掘、分布式安全查询、几何计算、科学计算等。在分布式环境下，具体应用通常会依赖于数据的存储模式和站点(Site)的可信度及其行为。

分布式应用通常采用两种模式存储数据：水平划分(Horizontally Partitioned)的数据模式和垂直划分(Vertically Partitioned)的数据模式。水平划分数据是将数据记录存储到分布式环境中的多个站点，所有站点存储的数据不重复；垂直划分数据是指分布式环境中每个站点只存储部分属性的数据，所有站点存储的数据不重复。

对分布式环境下的站点(参与者)，根据其行为可以分为准诚信攻击者(Semi-honest Adversary)和恶意攻击者(Malicious Adversary)。准诚信攻击者是遵守相关计算协议但仍试图进行攻击的站点；恶意攻击者是不遵守协议且试图披露隐私的站点。一般地，假设所有站点为准诚信攻击者。

1. 安全多方计算

在众多分布环境下，基于隐私保护的数据挖掘应用都可以抽象为无信任第三方(Trusted Third Party)参与的 SMC 问题，即怎样使两个或多个站点通过某种协议完成计算后，每一方都只知道自己的输入数据和所有数据计算后的最终结果。

以在分布式下计算集合的并运算为例：假设有 N 个独立站点 $S_1, S_2, \cdots, S_N$，站点 S_i 拥有数据 D_i，这 N 个站点可以在不暴露每个站点具体数据情况下计算出来。

可以证明，由于采用了可交换加密技术的顺序无关性，在整个求集合并集的过程中，除了集合交集的大小和最终结果被披露外，没有其他私有信息泄露，所以该计算集合并运算的方法是安全的。

由于多数 SMC 都基于"准诚信模型"假设之上，因此应用范围有限。SCAMD(Secure Centralized Analysis of Multi-party Data)协议在去除该假设基础上，引入准诚信第三方来实现当站点都是恶意时进行安全多方计算；有些研究者提出抛弃传统分布式环境下对站点行为约束的假设，转而根据站点的动机，将站点分为弱恶意攻击者和强恶意攻击者，用可交换加密技术解决在分布环境下的信息共享问题。

2. 分布式匿名化

匿名化即是隐藏数据或数据来源。对大多数应用而言，首先需要对原始数据进行处理以保证敏感信息的安全；然后再在此基础上，进行数据挖掘、发布等操作。分布式环境下的数据匿名化，都面临在通信时如何既保证站点数据隐私又能收集到足够的信息，来实现利用率尽量大的数据匿名的问题。

分布式匿名化利用可交换加密在通信过程中隐藏原始信息，再构建完整的匿名表判断是否满足 k-匿名条件来实现。

在水平划分的数据环境中，可以通过引入第三方，利用满足以下性质的密钥来实现数据的 k-匿名化。每个站点加密私有数据并传递给第三方，当且仅当有 k 条数据记录的准标志

符属性值相同时,第三方的密钥才能解密这 k 条数据记录。

更一般地,不考虑数据的具体存储模式,一种能确保分布式环境下隐私安全的模型是 k-TTP(k-Trusted Third Party)。k-TTP 利用信任第三方,确保了当且仅当至少有 k 个站点的信息改变时,所有站点的相关统计信息才能被披露。k-TTP 模型的约束,使我们不能揭露少于 k 个站点的统计信息。

由于分布式固有的复杂性,实现分布式数据匿名化的主要挑战是解决数据分散、站点自治、安全通信等之间的矛盾和冲突。

3. 分布式关联规则挖掘

在分布式环境下,关联规则挖掘的关键是计算项集合的全局计数,加密技术能保证在计算项集合计数的同时,不会泄露隐私信息。

例如,在数据垂直划分的分布式环境中,需要解决的问题是:如何利用分布在不同站点的数据计算项集合(Item Set)计数,找出支持度大于阈值的频繁项集。此时,计算项集合计数的问题被简化为在保护隐私数据的同时,在不同站点间计算标量积的问题。已有计算标量积的方法包括引入随机向量进行安全计算或用随机数代替真实值,然后用代数方法进行计算等。

4. 分布式聚类

基于隐私保护的分布式聚类的关键是安全地计算数据间的距离,有以下两种常用模型:

1) Naive 聚类模型

各个站点将数据用加密安全的信道传递给信任第三方,再由信任第三方进行聚类后返回结果。

2) 多次聚类模型

首先各个站点对本地数据进行聚类并发布结果,再通过对各个站点发布的结果进行二次处理,实现分布式聚类。

无论哪种分布式聚类模型,都利用了加密技术以实现信息的安全传输。当然,还有基于隐私保护的其他分布式聚类方法,如在任意划分数据的环境下的 k-mean 聚类算法,通过引入随机数来保证安全传输的最大期望(Expectation Maximization)聚类算法等。

6.4.4 基于限制发布的隐私保护技术

限制发布即是有选择的发布原始数据、不发布或者发布精度较低的敏感数据,以实现隐私保护。这类技术研究的重点是"数据匿名化",即在隐私披露风险和数据精度间进行折中,有选择地发布敏感数据及可能披露敏感数据的信息,但保证对敏感数据及隐私的披露风险在可容忍范围内。

数据匿名化一般采用两种基本操作,即抑制和泛化。

抑制是抑制某数据项,即不发布该数据项;泛化则是对数据进行更概括、抽象的描述。比如,对整数 5 的一种泛化形式是[3,6],因为 5 在区间[3,6]内。

1. 数据匿名化的原则

数据匿名化所处理的原始数据，如医疗数据、统计数据等，一般为数据表形式。表中每一条记录(或每一行)对应一个个人，包含多个属性值。这些属性可以分为如下三类。

(1) 显式标识符(Explicit Identifier)：能唯一标识单一个体的属性，如身份证号码、姓名等。

(2) 准标识符(Quasi-Identifiers)：联合起来能唯一标识一个人的多个属性，如邮编、生日、性别等联合起来则可能是准标识符。

(3) 敏感属性(Sensitive Attribute)：包含隐私数据的属性，如疾病、薪资等。

例如，如表 6-2 所示为一原始医疗数据，每一条记录对应一个唯一的病人，其中{“姓名”}为显式标识符属性，{“年龄”，“性别”，“邮编”}为准标识符属性，{“疾病”}为敏感属性。如表 6-3 所示则是匿名化数据。

表 6-2 原始数据

姓名	年龄	性别	邮编	疾病
Andy	4	M	12000	胃溃疡
Bill	5	M	14000	消化不良
Ken	6	M	18000	肺炎
Nash	9	M	19000	支气管炎
Alice	12	F	22000	流感
Betty	19	F	24000	肺炎

表 6-3 匿名化数据

年龄	性别	邮编	疾病
[1,5]	M	[10k,15k]	胃溃疡
[1,5]	M	[10k,15k]	消化不良
[6,10]	M	[15k,20k]	肺炎
[6,10]	M	[15k,20k]	支气管炎
[11,20]	F	[20k,25k]	流感
[11,20]	F	[20k,25k]	肺炎

2. *k*-匿名

Samarati 和 Sweeney 提出的 k-匿名原则要求所发布的数据表中的每一条记录不能区分于其他 $k-1$ 条记录。我们称不能相互区分的 k 条记录为一个等价类(Equivalence Class)。这里的不能区分只对非敏感属性项而言。一般 k 值越大，对隐私的保护效果更好，但丢失的信息越多。

k-匿名的缺陷在于没有对敏感数据做任何约束，攻击者可以利用一致性攻击(Homogeneity Attack)和背景知识攻击(Background Knowledge Attack)来确认敏感数据与个人的联系，导致隐私泄露。(α,k)-匿名原则在此基础上进行了改进，其在保证发布的数据满足 k-匿名化原则的同时，还保证发布数据的每一个等价类中，与任一敏感属性值相关

的记录的百分比不高于 α。

3. *l*-diversity

l-diversity 保证每一个等价类的敏感属性至少有 l 个不同的值。*l*-diversity 使得攻击者最多以 $1/l$ 的概率确认某个体的敏感信息。同样，在 2-diversity 中，每一个等价类中至少有 2 个不同的敏感属性值。另外，*l*-diversity 还有两种其他的形式：

1）基于熵的 *l*-diversity

如果每个等价类的熵 $\text{Entropy}(E) > \log l$，那么所发布的数据满足基于熵的 *l*-diversity。其中，等价类的熵定义为：

$$\text{Entropy}(E) = -\sum_{s \in S} p(E,s)\log p(E,s)$$

$p(E,s)$为等价类 E 中敏感属性值为 s 的记录的百分比。熵越大，表示等价类的敏感属性值分布越均匀，攻击者揭露个人的隐私就越困难。

2）递归(c,l)-diversity

如果每个等价类都满足 $r_1 < c(r_l + r_{l+1} + \cdots + r_m)$，那么就说所发布的数据满足递归$(c, l)$-diversity。这里，$r_i$ 表示该等价类中第 i 频繁的敏感属性值的个数。递归(c, l)-diversity 保证了等价类中频率最高的敏感属性值不至于出现频度太高。

4. t-Closeness

t-Closeness 在 *l*-diversity 基础上，考虑了的敏感属性的分布问题，它要求所有等价类中敏感属性值的分布尽量接近该属性的全局分布。

t-Closeness 的定义：令 $P=\{p_1, p_2, \cdots, p_m\}$，$Q_i=\{q_1, q_2, \cdots, q_m\}$分别表示各敏感值的全局分布和在等价类 C_i 中的分布。对任意等价类 C_i，若 P 与 Q_i 的距离 $D[P, Q_i]$满足公式：

$$D[P, Q_i] < t$$

则发布的数据满足匿名化原则 *t*-Closeness。其中，阈值 $t \in [0,1]$；度量距离可采用可变距离或 KL 距离。

除以上匿名化原则外，也有学者提出了个性化隐私保护（Personalized Privacy Preservation）的匿名化原则，以满足不同个人隐私保护的要求和级别，并克服了统一匿名化所造成的数据“过分”保护和保护“不足”。

一般来说，遵循 *k*-匿名、*l*-diversity 等匿名化原则发布数据都采用泛化技术，这在很大程度上降低了数据的精度和利用率。

一种改进的高精度的数据发布方法是 Anatomy：首先利用原始数据产生满足 *l*-diversity 原则的数据划分；然后将结果分成两张数据表发布，一张表包含每个记录的准标识符属性值和该记录的等价类 ID，另一张表包含等价类 ID、每个等价类的敏感属性值及其计数。这种将结果“切开”发布的方法，在提高准标识符属性数据精度的同时，保证了发布的数据满足 *l*-diversity 原则，对敏感数据提供了较好的保护。

5. 数据匿名化算法

数据匿名化场景如图 6-28 所示。

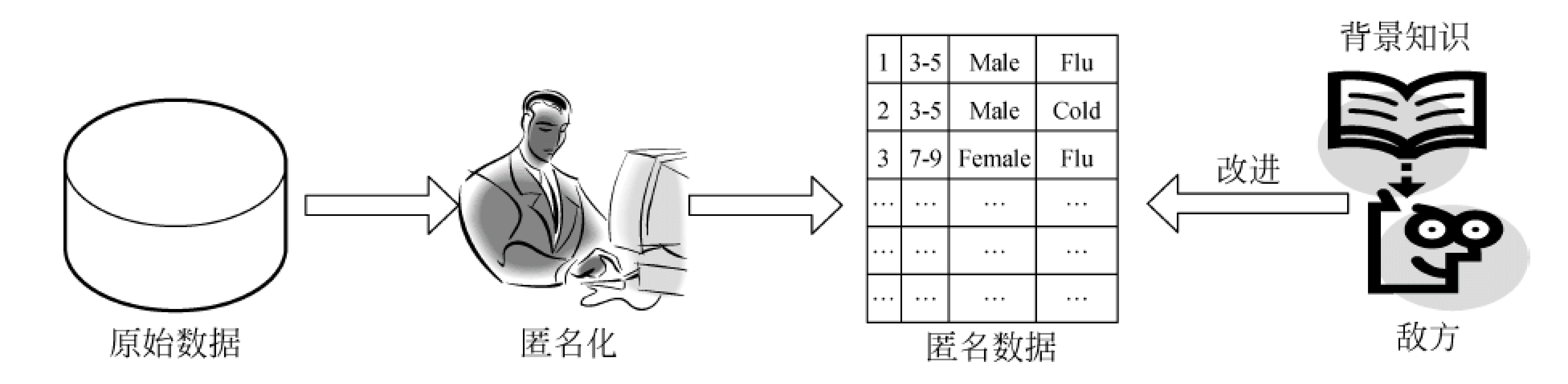


图 6-28 数据匿名化场景

大多数匿名化算法致力于解决根据通用匿名原则，怎样更好地发布匿名数据。另一部分工作致力于解决在具体应用背景下，如何使发布的匿名数据更有利于应用。因此，又出现采用聚类思想进行匿名化的算法，它能够在发布数据精度和计算开销间达到较好的平衡。

6. 基于通用原则的匿名化算法

不同情况下，实现 k-匿名的算法有多种度量可采用，如等价类所包含的平均记录条数、数据的信息缺损、实现数据匿名的操作数、可识别度量(Discernability Metrics)等。通常采用泛化(抑制)技术来实现最优化的 k-匿名原则的算法，对泛化空间(抑制策略)的搜索直接影响到了算法的性能。然而在很多简单限制条件下的最优化 k-匿名问题已经被证明是 NP-hard，因此，很大一部分实现 k-匿名的算法研究着眼于设计高效的近似算法。

如图 6-29 所示，基于通用原则的匿名化算法常包括泛化空间枚举、空间修剪、选取最优泛化、结果判断与输出等步骤。例如，最早提出的 MinGen 算法采用的就是每一步都完全搜索泛化空间，选出最优的泛化操作，一直进行这样的操作直到数据满足 k-匿名原则。但 MinGen 算法由于采用完全搜索，时间复杂度高，因此并不实用。Datafly 算法在 MinGen 算法的基础上，引入抑制与启发式泛化指导原则对效率进行了提升。

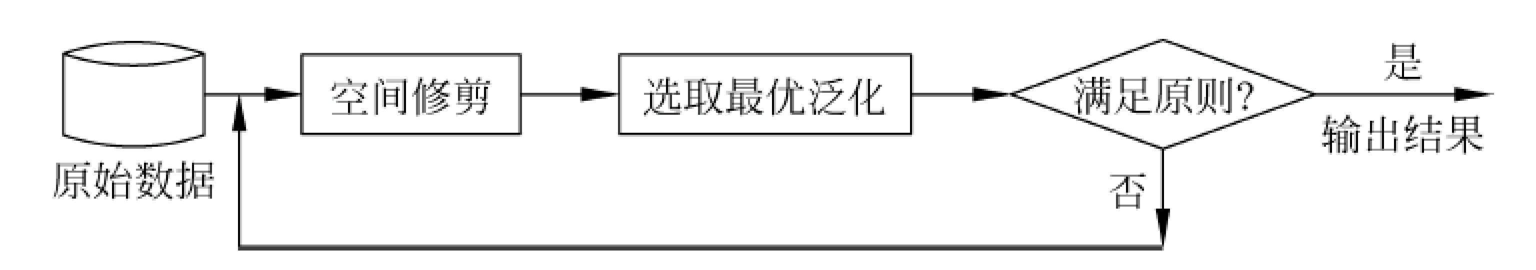


图 6-29 匿名算法流程

另一种广泛应用的 k-匿名算法是 Incognito，它首先构建包含所有全域泛化(一种全局重编码技术)方案的泛化图(Generalization Graph)，然后自底向上对原始数据进行泛化，每次选取最优泛化方案前，预先对泛化图进行修剪以缩小搜索范围，不断进行以上操作直到数据满足 k-匿名原则。其他优化的 k-匿名算法基本上也是采用修剪泛化空间来提升性能。

多维 k-匿名算法能够发布精度较高的数据，它将原始数据映射到一个多维空间，k-匿名问题即转换为在空间中对多维数据进行最优化划分的问题。

其他的匿名化原则算法，大多是基于 k-匿名算法，不同之处在于判断算法结束的条件，而泛化策略、对搜索空间的修剪等都是基本相同的。

7. 面向特定目标的匿名化算法

在特定的应用场景下，通用的匿名化算法可能不能满足特定目标的要求，因此需要设计具有针对性的匿名化算法。例如，考虑到数据应用者需要利用发布的匿名数据构建分类器，那么设计匿名化算法时就需要考虑在保护隐私的同时，怎样使发布的数据更有利于分类器的构建，并且采用的度量指标要能直接反映出对分类器构建的影响。已有的自底向上的匿名化算法和自顶向下的匿名化算法都采用了信息增益(Information Gain)作为度量。因为发布的数据信息丢失越少，构建的分类器的分类效果将越好。自底向上的匿名化算法通过每一次搜索泛化空间，采用使信息丢失最少的泛化方案进行泛化，重复执行以上操作直到数据满足匿名原则的要求。自顶向下的匿名化算法的操作过程与之相反。

类似地，针对以发布数据利用率最大化为特定目标的应用，有研究者提出了 Anonymized Marginals 信息发布方法；针对以防止关联规则推导为首要目标的应用，需要采用抑制，不发布能最大化降低关联规则支持度和置信度的属性值，从而破坏关联规则推导攻击；当发布的信息是多个视图时，也有研究者提出了保证发布的信息满足 k-匿名原则的算法。

8. 基于聚类的匿名化算法

基于聚类的匿名化算法将原始记录映射到特定度量空间中，再对空间中的点进行聚类来实现数据匿名。类似于 k-匿名，算法保证每个聚类中至少有 k 个数据点。

根据度量的不同，有研究者提出了 r-gather 和 r-cellular 这两种聚类算法。以 r-gather 算法为例，它以所有聚类中的最大半径为度量，需要达到的目标是对所有数据点进行聚类，在保证每个聚类至少包含 k 个数据点的同时，也使所有聚类中的最大半径越小越好。由于发布的结果只包含聚类中心、半径以及相关的敏感属性值，同一个等价类中的记录不可区分，因此对个人的敏感信息实现了隐藏。

基于聚类的匿名化算法主要面临两个挑战：

(1) 怎样对原始数据的不同属性进行加权？因为对属性的度量越准确，那么聚类的效果就越好；

(2) 怎样将不同性质的属性统一映射到同一个度量空间中。

9. 动态环境下的数据匿名化算法

以上所提到数据匿名化算法，都是针对静态数据而言，并未考虑数据动态变化时带来的挑战。而在动态环境下，数据通常会随时间的推移增加或减少，数据发布要求也会不相同。在动态环境下直接应用基于静态数据的匿名化算法，虽然在某一时刻发布的匿名化数据能很好地保护隐私，但是攻击者通过利用多个时刻发布的数据进行联合攻击，很容易获取敏感信息。

1) 基于动态递增数据的多次发布

考虑到现实生活中很多情况是数据不断地增加(如医院所拥有的病例信息)，提出并解决了基于动态递增数据的多次发布问题。

假设原始数据为 T，关于 T 的一系列增量更新为 $\Delta T_1, \Delta T_2, \cdots$。令根据 T 与前 i 次的增量更新发布的数据，其中 f_i 为匿名算法。当同时满足以下 3 个条件时，一系列发布对数据实现了 k-匿名隐藏。

(1) T^* 是 k-匿名化的：$T^* = f(T)$。

(2) $\forall i \geqslant 1, T_i^*$ 是 k-匿名化的。

(3) 对每个非空整数集$\{i_1, i_2, \cdots, i_n\}$，推导表 $I(f_{i_1}(T_1), \cdots, f_{i_n}(T_n))$也是 k-匿名化的。

问题的复杂性在于：不仅要保证每一次单独发布数据的匿名化，而且要保证即使通过联合多次发布的数据进行攻击，隐私仍然能够得到保护。

2) 基于"攻击检测与防止"的方法

首先对当前的数据进行匿名化处理，然后再检测是否有攻击联合先前发布的数据而披露隐私。直到没有攻击能够披露数据隐私时则停止对数据的进一步匿名化。

只有增量更新的数据集被称为"准动态"数据集，同时有数据增加和减少的数据集则称为动态数据集。提出了一种在动态环境下保护隐私的匿名化原则 m-Invariance。假设 $T*(1), \cdots, T*(n)$是在动态环境下先后发布的一系列数据，我们称这一系列发布的数据满足 m-Invariance 匿名化原则，当且仅当同时满足：

(1) 对 i 时刻发布的数据 $T*(i)$，其每一个等价类中都至少有 m 条记录且这些记录都有不同敏感属性值；

(2) 如果某条记录出现在不同时刻的多次发布中，那么每一次发布这条记录所在的等价类包含的敏感属性值形成的集合须相等。

第一个条件保证了每个时刻发布的数据的隐私披露风险不会高于 $1/m$，同时两个条件联合起来保证攻击者利用多次发布的数据进行攻击时，不会披露新增加和已经减少的数据的隐私。

满足 m-Invariance 匿名化原则的数据发布算法如下：

(1) 首先将前后两次共有的数据分配到包含相同的敏感属性值集合的等价类中；

(2) 然后尝试将新增加的记录分配到这些等价类中，同时保证剩下的未分配的数据满足可以形成第 1 个条件的等价类；

(3) 为剩下未分配的数据建立新的等价类；最后对过大、可以分裂的等价类进行调整。

除了数据的插入、删除会引起数据的动态变化外，每条记录属性值的更新，同样会导致数据动态变化。

其假设敏感属性值由始终不变和随机动态变化两种组成。对后者而言，由于其随时间是随机变化的，对其进行多次发布不会带来新的威胁；而对始终不变(Permanent)的敏感属性值而言，如果在多次发布中不考虑它不变的特点，将变得不再安全。因此，该问题的关键在于如何实现不变敏感属性值的匿名发布。

数据匿名化由于能处理多种类型的数据，并发布真实的数据，能满足众多实际应用的需求，因此受到广泛关注。由此可见，数据匿名化是一个复杂的过程，需要同时权衡原始数据、匿名数据、背景知识、匿名化技术、攻击等众多因素。

总之，每类隐私保护技术都有不同的特点，在不同应用需求下，它们的适用范围、性能表现等不尽相同。当针对特定数据实现隐私保护且对计算开销要求比较高时，基于数据失真的隐私保护技术更加适合；当更关注于对隐私的保护甚至要求实现完美保护时，则应该考虑基于数据加密的隐私保护技术，但代价是较高的计算开销(在分布式环境下，还会增加通信开销)。而数据匿名化技术在各方面都比较平衡，即能以较低的计算开销和信息缺损实现对隐私保护。

6.5 位置隐私保护

基于位置的服务(Location-Based Service,LBS)是指通过无线通信和定位技术获得移动终端的位置信息(如经纬度的坐标数据),将此信息提供给移动用户本人或他人或应用系统,以实现各种与当前用户位置相关的服务并提供给移动用户本人。

近年来,随着移动通信设备和无线通信技术的快速发展,定位技术的不断成熟以及服务与内容提供商的不断增加,LBS 呈现出迅猛增长的态势。然而,在 LBS 服务中,由于用户的位置频繁变换,LBS 必须不间断地跟踪用户当前所在位置,导致用户的位置信息越来越多地暴露给 LBS 服务提供商,使得将用户位置信息作为用户个人的隐私信息得到保护变得更加重要。研究表明,位置信息能否得到妥善的保护,将成为影响 LBS 服务得到进一步推广和普及的关键因素之一。LBS 服务中对用户隐私信息的保护成为亟待解决的问题。

位置隐私保护不是指要保护用户的个人信息不被他人使用,而是指用户对个人的位置信息进行有效控制的权利。位置信息是一种特殊的个人隐私信息,对其进行保护就是要给予所涉及的个人决定和控制自己所处位置的信息何时、如何及在何种程度上被他人获知的权利。因此,按照对用户隐私信息进行保护的要求,LBS 服务提供商必须为用户提供一种完全由用户本人控制其位置信息能否被他人获取的方式,使得用户可以自行决定在何种环境下将其位置信息告知何人。

目前,已有多种针对 LBS 中用户位置信息的隐私保护方法,如通过立法或行业规范的方式进行保护、通过匿名的方式进行保护、通过区域模糊的方式进行保护、通过隐私策略的方式进行保护等。由于隐私信息的保护被视为用户对个人隐私信息的访问和使用提供有效控制的权利和手段,再加上个人对隐私保护需求的不同,因此用户分别设置相应的隐私策略来保护个人的隐私,成为目前众多隐私信息保护方法中最有效的方法之一。另外,在某些 LBS 服务中,对一个用户的位置信息的访问可能需要被多个用户同时控制。例如,家长可以使用 GPS 设备通过提供的 LBS 服务跟踪孩子的位置,以确保孩子的安全。家长有权利控制孩子的位置信息被他人访问,同时有必要提供必须获得父母双方授权才能访问孩子位置信息的机制,以达到更灵活、更完善地进行保护的目的。因此,隐私保护方法必须能方便、灵活地满足在所有的情况下每个用户对隐私保护的不同需求。

针对上面所述亟待解决的用户位置隐私保护问题,何泾沙等学者提出了一种面向隐私保护的访问控制模型,用于支持用户灵活地设置隐私策略,实现对 LBS 服务中用户位置信息的隐私进行有效的保护。

6.5.1 面向隐私保护的访问控制模型

面向隐私保护的访问控制模型是一个基于三维访问控制的矩阵,是对传统的面向安全保护的二维访问控制矩阵的扩展,目的是更好地保护用户的位置隐私信息。

传统的二维访问控制矩阵是实现访问控制机制的经典的安全模型。在该模型中,可以在一个二维访问控制矩阵 $\boldsymbol{M}$ 中设定任意主体 s(即 LBS 服务用户)对任意客体 o(即位置信息)的访问权限 r。因此,矩阵 $\boldsymbol{M}$ 是一个由 p 个主体和 q 个客体组成的二维矩阵,$\boldsymbol{M}$ 中的每

一行代表某个主体对所有系统中的客体进行访问的权限属性；$\boldsymbol{M}$ 中的每一列代表某个客体被所有系统中的主体访问的权限属性，$\boldsymbol{M}$ 中每一个矩阵元素 $\boldsymbol{M}[s,o]$ 的内容为所在行的主体 s 对所在列的客体 o 的访问权限设置。系统中访问控制机制的任务就是确保任何主体对客体的访问请求都是按照访问控制矩阵中主体对客体的访问权限的设置来确定是否授权访问请求。

为了满足对隐私信息进行保护的特殊需要，对以上传统的二维访问控制矩阵进行扩充。不同于面向安全的信息保护，隐私保护的特点是信息的隐私属性不能独立定义，而是与主体相关联，即信息的隐私属性取决于 1 个或多个相关联的具体的主体。对于某些主体来说，认为是隐私的信息对于其他主体来说却并不是隐私，同时 1 份隐私信息可能涉及多于 1 个与该信息相关联的主体。例如，1 份公司的项目文件可能包含与公司内部多个部门相关联的商业机密信息，因此，这些部门的负责人都应该拥有控制用户对这份文件进行访问的能力。

为了反映隐私信息的特点，满足对隐私信息进行保护的需要，引入隐私相关者的概念。隐私相关者是指 1 份信息中所包含的涉及隐私的所有相关用户，因此，对这份信息的未授权访问会侵犯这些用户的隐私。由于一份信息可以对应多个隐私相关者，因此针对这个特点和要求，将隐私相关者加入到传统的访问控制模型中，在传统的二维访问控制矩阵的基础上增加 1 个维度来表达隐私相关者对访问请求实施控制的能力。扩充后的面向隐私保护的访问控制模型基于 1 个三维访问控制矩阵，可以用来使所有隐私相关者共同控制对 1 份涉及他们隐私信息的访问，由此来达到保护用户隐私的目的。

在新的三维访问控制矩阵中，由主体（即提出访问请求的用户）、客体（即隐私信息）和隐私相关者（即隐私信息所涉及的相关用户）这 3 个因素共同确定主体是否拥有对客体的访问权限。三维访问控制矩阵 $\boldsymbol{M}$ 中的第一维 $\boldsymbol{S}(s\in\boldsymbol{S})$ 代表主体的集合、第二维 $\boldsymbol{O}(o\in\boldsymbol{O})$ 代表客体的集合、第三维 $\boldsymbol{S}'(s'\in\boldsymbol{S}')$ 代表隐私相关者的集合。该三维矩阵中的元素 $\boldsymbol{M}[s,o,s']$ 表达信息 o 的隐私相关者 s' 赋予信息请求者 s 对隐私信息 o 的访问权限，其访问控制的基本规则如下：

(1) 若 $\boldsymbol{M}[s,o,s']$ 中的内容为空，表示 s' 并不是隐私信息 o 的隐私相关者，对 o 进行访问不需要得到 s' 的任何授权。

(2) 若对所有 $s'(s'\in\boldsymbol{S}')$，$\boldsymbol{M}[s,o,s']$ 中的内容均不包含某特定的访问权限，表示 s 对 o 没有该特定的访问权限。

(3) 若对任意 $s'(s'\in\boldsymbol{S}')$，$\boldsymbol{M}[s,o,s']$ 中的内容包含有 < “访问权限”,“不允许” >，表示 s 对 o 没有该“访问权限”。

在以上的三维访问控制矩阵模型中，每一个 $\boldsymbol{M}[s,o,s']$ 中的内容或者为空，或者为隐私相关者 s' 授权主体 s 对客体 o 的一种或多种访问权限的设置，如读 read、写 write、执行 execute 等。如果主体 s 请求对客体 o 进行 r 访问，该访问请求必须得到客体 o 的所有隐私相关者 $s'i$ $(s'i\in\boldsymbol{S}')$ 的授权才允许执行，即所有 o 的隐私相关者 $s'1, s'2, \cdots, s'k$ $(s'i\in\boldsymbol{S}')$ 所对应的矩阵元素 $\boldsymbol{M}[s,o,s'1]$, $\boldsymbol{M}[s,o,s'2]$, $\cdots$, $\boldsymbol{M}[s,o,s'k]$ 中都必须包含访问权限 < “r”,“允许” >。确定客体 o 的所有隐私相关者 $s'1, s'2, \cdots, s'k$ $(s'i\in\boldsymbol{S}')$ 及是否授权访问的基本规则如下：

(1) 查看所有 $s'(s'\in\boldsymbol{S}')$ 对应的矩阵元素 $\boldsymbol{M}[s,o,s']$，若 $\boldsymbol{M}[s,o,s']$ 的内容中包含 < “r”,“允许” > 或 < “r”,“不允许” >，则表明 s' 为 o 的隐私相关者；由此可以确定客体 o 的

所有隐私相关者 $s'1, s'2, \cdots, s'k$ （$s'i \in \boldsymbol{S}'$）。

(2) 若对于所有 $s'i$ （$s'i \in \boldsymbol{S}', 1 \leqslant i \leqslant k$），在 $\boldsymbol{M}[s, o, s'i]$（$1 \leqslant i \leqslant k$）中存在至少 1 个访问权限设置<"$r$"，"不允许">，则拒绝访问请求 r。此时 $\boldsymbol{M}[s, o, s'i]$ 中的<"r"，"不允许">意味着 o 的隐私相关者 $s'i$ 明确拒绝 s 对 o 进行 r 访问。

为了满足不同环境下对隐私保护的需求，三维访问控制模型允许设置其他更加灵活的访问权限及授权方式。例如可以设置若半数以上的隐私相关者允许访问，则授权访问请求，或更加通用地设置若 n 个隐私相关者中至少有 m 个隐私相关者允许访问，则授权访问请求。

在以上的解释中，授权的原则是：只要有任何隐私相关者不允许访问，则拒绝该访问请求，这样做可以最大化地保护用户的隐私信息。

6.5.2 LBS 服务中的位置隐私信息保护

三维访问控制模型可以用于对 LBS 服务中的用户位置隐私进行保护。整个位置隐私保护的过程可以分为两个部分：访问权限设置和访问控制决策。

首先，所有某一位置信息相关的隐私相关者设置相对于该位置信息对所有信息请求者的访问权限。通过权限的设置，隐私相关者可以设置哪些信息请求者、可以在什么环境下(如时间、地点等)获取该位置信息的全部或某些部分。例如，在每天的 8:00～17:00，当位置信息的隐私相关者在北京王府井时，允许某些请求者得知其所在的精确位置信息，即北京市东城区王府井步行街王府井百货 6 楼；而对另外一些请求者，只允许得知其所在的大概位置是在北京。

第二，在访问控制矩阵中设置了所有的权限之后，访问决策部分对访问请求者提出的具体的访问请求按照矩阵中的设置做出具体的允许或拒绝访问的决策。在每次信息访问请求者提出访问位置信息的请求时，系统中的访问控制决策机制将查询设置在三维访问控制矩阵中的隐私权限，并根据隐私权限确定允许或拒绝访问请求。

分析在一个 LBS 典型服务中的场景：母亲为孩子的安全，让孩子随身携带一个定位设备(如智能手环或手机)，可以随时了解孩子所处的位置。这是最常见的应用场景，因为很多研究表明，孩子的家长更加倾向于使用定位服务。同时，出于保护孩子安全的考虑，母亲并不希望任何其他人都可以获得孩子的位置信息，但却希望孩子的老师在某些特定的情况下获知孩子的位置信息。因此，需要为此设置访问控制策略及权限，以决定什么人能够在什么时候、什么情况下访问孩子的位置信息。由于孩子是未成年人，没有能力制定最合适的访问策略，他们的安全由家长来负责，因此母亲就成为孩子位置信息的隐私相关者，负责制定相关的访问控制策略，保护孩子的位置隐私信息。

在允许母亲在任何时间、任何情况下都可以查询孩子位置信息的要求下，在访问控制模型的三维矩阵中，所对应的主体为母亲、所对应的客体为孩子位置信息的矩阵元素 $\boldsymbol{M}$[母亲，孩子位置信息，s']（$s' \in \boldsymbol{S}'$）中，访问权限均可设置为<"读"，"允许">，因此，母亲可以任意获取包含孩子位置信息的文件。

此外，孩子的父亲也希望与母亲一同来控制对孩子位置信息的访问，以更好地保护孩子的隐私。有些访问请求需要父母亲双方的授权才允许执行，任何对孩子位置信息未经授权的访问都可以被视为是对父母亲隐私的侵犯，父母亲双方都成为孩子位置信息的隐私相关者。

在 LBS 位置服务中，对客体(即孩子位置信息)的访问需要得到所有隐私相关者(即父

亲和母亲双方)的授权。

首先,父母确定何人可以访问孩子位置信息,以此确定允许访问存放孩子位置信息的文件作为客体的主体。

然后,在分别由父亲和母亲作为隐私相关者的2个矩阵元素中设置"读"权限。例如,如果在所对应的2个矩阵元素中均设置了如下的权限:<"读","询问">,即在该矩阵元素所对应的主体请求访问孩子位置信息时,需要立即"询问"父亲和母亲,以获得父母亲的实时授权。在这种情况下,只有当对父母双方的实时询问都得到访问授权时,才允许访问请求者读取孩子位置信息的文件。对于任何隐私相关者未设置相关权限的主体,都不能访问作为客体的孩子位置信息的文件。

为了描述提供LBS位置服务的服务器在接收到位置信息查询的请求时,做出访问控制决策的过程,假设用户 s 请求访问存放孩子位置信息的文件 o,服务器在接收到 s 的访问请求后,由访问控制机制通过以下的过程进行访问控制决策:

(1) 检索三维访问控制矩阵中对应于主体 s 和客体 o 的所有矩阵元素 $\boldsymbol{M}[s,o,s']$($s'\in \boldsymbol{S}'$),获取所有矩阵元素 $\boldsymbol{M}[s,o,s']$($s'\in \boldsymbol{S}'$)的内容。

(2) 检测所有 $\boldsymbol{M}[s,o,s']$($s'\in \boldsymbol{S}'$)的内容中是否包含"读"权限,如<"读","…">。

(3) 如果检索结果为空,即没有任何矩阵元素包含"读"权限,则拒绝此访问请求,即父母亲不允许信息请求者 s 访问包含孩子位置信息的文件 o。

(4) 如果检索结果不为空,即矩阵元素 $\boldsymbol{M}[s,o,$母亲$]$或 $\boldsymbol{M}[s,o,$父亲$]$中至少有一个包含的内容有<"读","…">,如果有任何矩阵元素的内容为<"读","不允许">,则拒绝此访问请求,即父亲或母亲不允许信息请求者 s 访问包含孩子位置信息的文件 o。

(5) 根据矩阵元素 $\boldsymbol{M}[s,o,$母亲$]$和 $\boldsymbol{M}[s,o,$父亲$]$中的内容,如果 $\boldsymbol{M}[s,o,$母亲$]$和 $\boldsymbol{M}[s,o,$父亲$]$的内容均为<"读","允许">,则授权此访问请求;如果矩阵元素 $\boldsymbol{M}[s,o,$母亲$]$或 $\boldsymbol{M}[s,o,$父亲$]$中包含内容<"读","询问">,则向母亲或父亲发送实时位置信息访问请求,然后等待母亲或父亲的实时决策,在向父母亲发送访问请求询问时,访问控制机制会将相关信息(如信息请求者 s、当前时间以及目前孩子所处的位置等)同时发送给父母亲,父母亲根据以上综合信息做出允许或者拒绝访问的决策,并将决策结果传回访问控制机制,由访问控制机制根据决策原则做出访问控制决策。

从以上过程可以看出,所有隐私相关者(如本例中的父母亲)可以同时控制信息请求者对隐私信息的访问。此外,模型可以灵活地增加隐私相关者的人数,即所有与某份隐私信息相关的用户均可以对该隐私信息的访问进行控制。即面向隐私保护的访问控制模型对隐私相关者的数量没有限制,可以满足LBS服务中对隐私信息进行灵活保护的要求。

6.6 轨迹隐私保护

6.6.1 轨迹隐私保护概述

1. 轨迹隐私保护的概念

轨迹隐私是一种特殊的个人隐私,它是指个人运行轨迹本身含有的敏感信息(如访问过

的敏感位置)，或者由运行轨迹推导出的其他个人信息(如家庭住址、工作地点、生活习惯、健康状况等)。因此，轨迹隐私保护既要保证轨迹本身的敏感信息不泄露，又要防止攻击者通过轨迹推导出其他的个人信息。

2. 轨迹隐私保护技术大致可以分为以下3类：

1）基于假数据的轨迹隐私保护技术

它是指通过添加假轨迹对原始数据进行干扰，同时又要保证被干扰的轨迹数据的某些统计属性不发生严重失真。

2）基于泛化法的轨迹隐私保护技术

该技术是指将轨迹上所有的采样点都泛化为对应的匿名区域，以达到隐私保护的目的。

3）基于抑制法的轨迹隐私保护技术

它是指根据具体情况有条件的发布轨迹数据，不发布轨迹上的某些敏感位置或频繁访问的位置以实现隐私保护。

假数据轨迹隐私保护方法简单、计算量小，但易造成假数据的存储量大及数据可用性降低等缺点；基于泛化法的轨迹隐私保护技术可以保证数据都是真实的，然而计算开销较大；基于抑制法的轨迹隐私保护技术限制发布某些敏感数据，实现简单，但信息丢失较大。目前，基于泛化法的轨迹 k-匿名技术(Trajectory k-anonymity)在隐私保护度和数据可用性上取得了较好的平衡，是目前轨迹隐私保护的主流方法。

3. 轨迹隐私保护度量标准

在轨迹数据发布中，由于发布后的数据要供第三方分析和使用，隐私保护技术要在保护轨迹隐私的同时有较高的数据可用性；在基于位置的服务中，隐私保护技术既要保护移动对象的轨迹隐私，又要保证移动用户获得较高的服务质量。

总的来说，轨迹隐私保护技术的度量标准包括两个方面：

1）隐私保护度

一般通过轨迹隐私的披露风险来反映，披露风险越小，隐私保护度越高。披露风险是指在一定情况下，轨迹隐私泄露的概率。披露风险与隐私保护算法的好坏和攻击者掌握的背景知识有很大的关联。攻击者掌握的背景知识越多，披露风险越高。在轨迹隐私保护中，攻击者掌握的背景知识可能是在空间中移动对象的分布情况、移动对象的运行速度、该区域的道路网络情况等。

2）数据质量/服务质量

在轨迹数据发布中，数据质量是指发布数据的可用性，数据的可用性越高，数据质量越好。一般采用信息丢失率(又称为信息扭曲度)来衡量数据质量的好坏。在基于位置的服务中，采用服务质量来衡量隐私保护算法的好坏，在相同的隐私保护度下，移动对象获得的服务质量越高则隐私保护技术越成熟。一般情况下，服务质量由响应时间、查询结果的准确性来衡量。

4. 轨迹隐私保护系统的结构

在基于位置的服务中，轨迹隐私保护系统的结构有分布式点对点结构和中心服务器结

构两种。分布式点对点结构由客户端和服务提供商两个部件组成,客户端之间通过 P2P 协议通信,判断客户端之间的距离,通过彼此协作完成隐私保护过程。中心服务器结构由客户端、服务提供商和匿名服务器三部分组成,如图 6-30 所示。

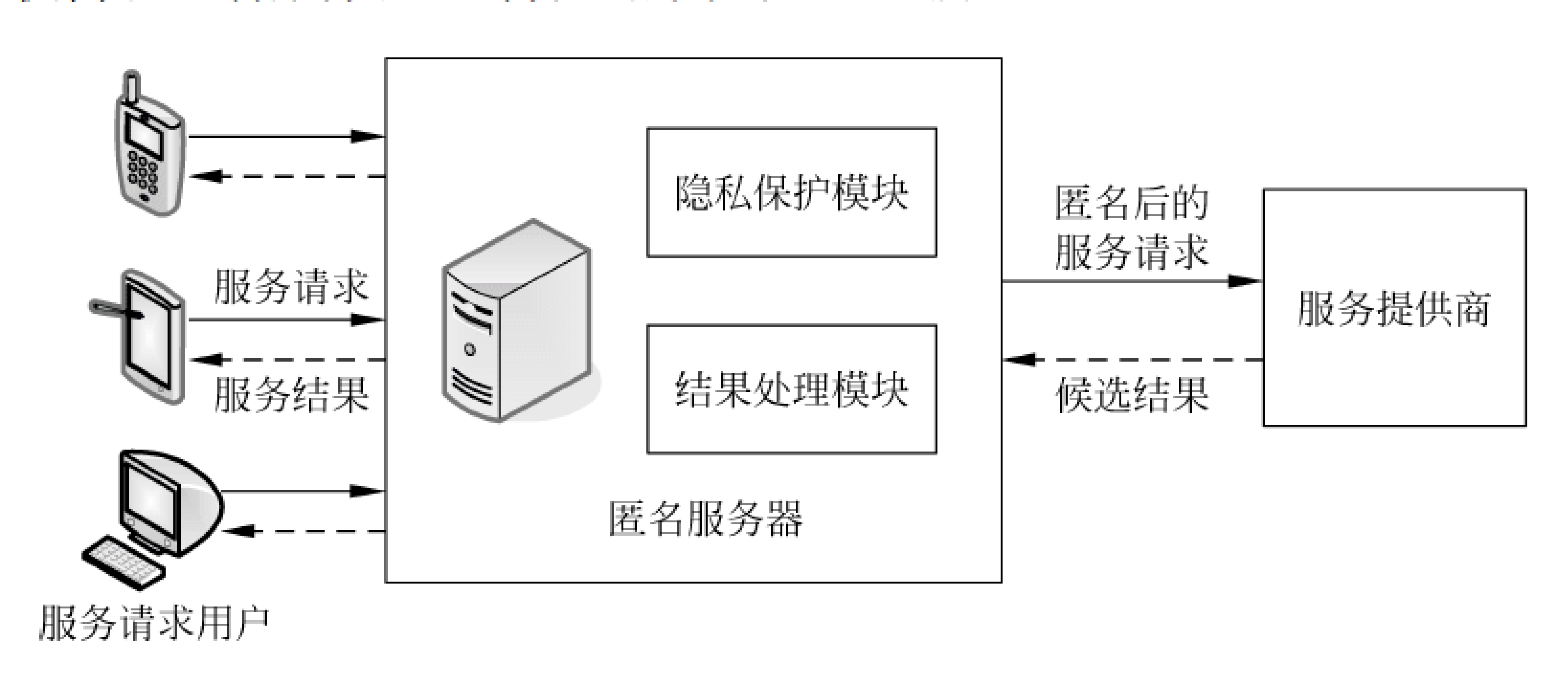


图 6-30 中心服务器结构

匿名服务器包含了隐私保护模块和结果处理模块。隐私保护模块负责收集客户端的位置、对客户端进行隐私保护处理;结果处理模块负责接受服务提供商发回的候选结果,对候选结果求精,并将最终结果返回给客户端。由于中心服务器结构具有容易实现、掌握全局数据等优点,已经成为目前最常用的系统结构。

在轨迹隐私保护技术度量标准和系统架构的基础上,以下分别对目前三种主流的轨迹隐私保护技术进行分析。

6.6.2 基于假数据的轨迹隐私保护技术

1. 假数据的轨迹隐私保护技术概述

在位置隐私保护技术中,假位置是经常使用的一种简单有效的技术。假位置即不发布真实位置,用假位置获得相应的服务。在轨迹数据隐私保护中,同样可以使用假轨迹方法。假轨迹方法通过为每条轨迹产生一些假轨迹来降低披露风险。例如,如表 6-4 所示存储了原始轨迹数据,移动对象 O_1、O_2、O_3 在 t_1、t_2、t_3 时刻的位置存储在数据库中,形成了 3 条轨迹。

表 6-4 原始数据

MOB	t_1	t_2	t_3
O_1	(1,2)	(3,3)	(5,3)
O_2	(2,3)	(2,7)	(3,8)
O_3	(1,4)	(3,6)	(5,8)

如表 6-5 所示是对原始数据进行假数据扰动后的结果。I_1、I_2、I_3 分别是移动对象 O_1、O_2、O_3 的假名;I_4、I_5、I_6 是生成的假轨迹的假名。经过假轨迹扰动后的数据库中含有 6 条假轨迹,每条真实轨迹的披露风险降为 1/2。简单地说,产生的假轨迹越多,披露风险就越低。

表 6-5　用假数据法干扰后的轨迹数据库

MOB	t_1	t_2	t_3
I_1	(1,2)	(3,3)	(5,3)
I_2	(2,3)	(2,7)	(3,8)
I_3	(1,4)	(3,6)	(5,8)
I_4	(1,1)	(2,2)	(3,3)
I_5	(2,4)	(2,6)	(4,6)
I_6	(1,3)	(2,5)	(3,7)

一般来说,假轨迹方法要考虑以下三个方面:

1）假轨迹的数量

假轨迹的数量越多,披露风险越低,但是同时对真实数据产生的影响也越大。因此,假轨迹的数量通常根据用户的隐私需求选择折中数值。

2）轨迹的空间关系

从攻击者的角度看,从交叉点出发的轨迹易于混淆,因此,应尽可能产生相交的轨迹以降低披露风险。

3）假轨迹的运动模式

假轨迹的运动模式要和真实轨迹的运动模式相近,不合常规的运动模式容易被攻击者识破。

2. 假数据的轨迹隐私保护的实现

针对上述 3 种要求,出现了两种生成假轨迹的方法,即随机模式生成法和旋转模式生成法。

1）随机模式生成法

随机生成一条连接起点到终点、连续运行且运行模式一致的假轨迹。

2）旋转模式生成法

以移动用户的真实轨迹为基础,以真实轨迹中的某些采样点为轴点进行旋转,旋转后的轨迹为生成的假轨迹。旋转点的选择和旋转角度的确定需要和信息扭曲度进行关联权衡。

旋转模式生成法生成的假轨迹与真实用户的运动模式相同,并和真实轨迹有交点,难以被攻击者识破。

6.6.3　基于泛化法的轨迹隐私保护技术

在轨迹隐私保护中,最常用的方法是轨迹 k-匿名技术。k-匿名模型主要应用在关系数据库的隐私保护中。其核心思想是将 QI 属性泛化,使得单条记录无法和其他 $k-1$ 条记录区分开来。Marco Gruteser 最先将 k-匿名技术应用到位置隐私保护中,产生了位置 k-匿名模型,即当移动对象在某一时刻的位置无法与其他 $k-1$ 个用户的位置相区别时,称此位置满足位置 k-匿名。随后,k-匿名模型也应用到轨迹隐私保护技术中,产生了轨迹 k-匿名。一般来说,k 值越大则隐私保护效果越好,然而丢失的信息也越多。

给定若干条轨迹,对于任意一条轨迹 T_i,当且仅当在任意采样时刻 t_i,至少有 $k-1$ 条轨迹在相应的采样位置上与 T_i泛化为同一区域时,称这些轨迹满足轨迹 k-匿名,满足轨迹

k-匿名的轨迹被称为在同一个k-匿名集中。采样位置的泛化区域(又称匿名区域)可以是最小边界矩形(MBR),也可以是最小边界圆形(MBC),可以根据具体需求进行调整。

下面的例子展示了轨迹k-匿名的概念。

如表 6-6 所示是对表 6-4 中的原始数据进行轨迹 3-匿名后的结果。

表 6-6　轨迹 3-匿名

MOB	t_1	t_2	t_3
I_1	[(1,2),(2,4)]	[(2,3), (3,7)]	[(3,5), (3,8)]
I_2	[(1,2),(2,4)]	[(2,3), (3,7)]	[(3,5), (3,8)]
I_3	[(1,2),(2,4)]	[(2,3), (3,7)]	[(3,5), (3,8)]

表 6-6 中的I_1、I_2和I_3分别是移动对象O_1、O_2、O_3的假名。3 个时刻的位置也泛化为 3 个移动对象的最小边界矩形。匿名区域采用左下角坐标和右上角坐标来表示。例如,[(1,2),(2,4)]表示左下角坐标为(1, 2),右上角坐标为(2, 4)的最小边界矩形。

在数据发布中和基于位置的服务中均有关于轨迹k-匿名技术的研究,两种场景下对轨迹k-匿名的侧重点不同,下面分别介绍两个场景中的轨迹k-匿名方法。

1. 数据发布中的轨迹 k-匿名

在轨迹数据发布的隐私保护中,轨迹k-匿名要将静态的轨迹数据库D转换为$D*$,使得$D*$中的任意一条轨迹T_i*都属于某个轨迹k-匿名集,且$D*$和D之间的信息扭曲度最小。在信息扭曲度最小的情况下达到轨迹k-匿名是 NP-hard 问题,其中有以下几个关键的研究问题。

1) QI 属性的识别

QI 属性又称为准标识符,它是指联合起来能唯一识别某个个体的多个属性的集合。例如,邮编、生日、性别等联合起来是准标识符。在关系数据隐私保护中,属性一般分为 QI 属性和敏感信息,隐私保护技术将 QI 属性泛化,使得发布的数据中每一条记录不能区分于其他k-1 条记录。然而在轨迹数据中,QI 属性与敏感信息很难界定,轨迹上任何位置或位置的集合都有可能成为区分于其他轨迹的 QI 属性。

例如,在某个时刻,T_i是唯一一个经过了位置L_i和L_j的轨迹,那么L_i和L_j就可以作为T_i的 QI 属性。

多数算法在保护轨迹数据隐私时,并不考虑 QI 属性与其他属性的区别,而是将整条轨迹上的任何一个采样点均做泛化处理;也有的方法从动态 QI 属性的角度出发进行隐私保护。所谓动态 QI 属性是指某条轨迹的 QI 属性在不同的时刻t_i由不同的位置组成。由于动态 QI 属性自身的特性,必须找到在所有时刻$t_1,\cdots,t_n$上距离O的聚集距离最小的$k-1$个对象,并将这k个对象匿名到一个匿名区域中以达到轨迹k-匿名。

2) 轨迹k-匿名集的形成

寻找轨迹k-匿名集的原则是使得 D * 与 D 的信息扭曲度尽可能小。因此,匿名集中的k条轨迹在时空上要尽可能地相近,即匿名集中的轨迹既要分布在相同的时间段内又要在空间距离上相近。为了能达到时间相近的目的,大多数算法都采用了预处理的方式,将分布在相同时间段内的轨迹放入同一个等价类中。然后,在同一个等价类中寻找空间距离相近的

轨迹 k-匿名集。寻找轨迹 k-匿名集的方法有两大类,一类是通过整条轨迹聚类找到距离相近的轨迹形成 k-匿名集;另一类是通过某条轨迹上最近邻采样点位置找到轨迹 k-匿名集。不管用何种方式,为了到达较小的信息扭曲度,都必须遵循 k 条轨迹之间距离尽可能小的原则。

3) 轨迹距离的计算

轨迹聚类或寻找最近邻采样点均需要计算轨迹或者采样位置之间的距离。目前,研究者们已经提出了多种轨迹距离的计算方法,比如欧几里得距离、编辑距离、最长共同序列距离、对数距离等。目前,大多数方法采用欧几里得距离计算轨迹或采样点之间的距离,也有的方法采用对数距离计算轨迹之间的距离。选择何种距离计算函数和信息扭曲度的衡量函数有直接关系。例如,如果信息扭曲度由数据库 D 和 D * 之间的欧几里得距离衡量,那么,相应的轨迹距离也应采用欧几里得距离。

2. LBS 中的轨迹 k-匿名

基于位置的服务是指服务提供商根据移动用户的位置信息提供各种服务。例如,紧急救援服务、基于位置的娱乐信息服务、生活信息服务以及基于位置的广告服务等。由于 LBS 服务与用户提出请求的位置有关,因此,使用基于位置的服务最大的隐私威胁就是位置隐私的泄露,也就是说,暴露用户的位置以及获知位置后用户收到的与时空相关的推理攻击。例如,用户不想让别人知道目前所在的位置(如酒吧)以及将要去的位置(如查询最近的宾馆等)。位置隐私保护技术的出现解决了这类问题,它可以保护移动用户在某个时刻的位置信息以及用户在发出连续查询时的位置信息。不过,更严重的问题是:保护了用户的位置隐私并不一定能保护用户的轨迹隐私。例如,通过位置隐私保护技术,移动对象在发出 LBS 请求的时刻均发布了一个匿名框,将这些匿名框连接起来,会暴露移动对象的大致轨迹。

在基于位置的服务中,轨迹 k-匿名与位置 k-匿名不同,轨迹 k-匿名要求任一条轨迹在起始点至终止点的所有采样位置都必须和相同的 $k-1$ 条轨迹匿名。基于位置的服务中的轨迹 k-匿名与数据发布中的轨迹 k-匿名不同,待匿名的轨迹数据不是静态的,而是动态变化的。因此,如何从轨迹起始时就能确定轨迹 k-匿名集是一个挑战性问题。在基于位置的服务中,轨迹 k-匿名集的方法大致有以下几种。

1) 基于轨迹划分的轨迹 k-匿名

将轨迹分片,对每个片段与其他轨迹的片段进行匿名,可以解决将整条轨迹匿名带来的不确定性问题,研究者提出了轨迹分片匿名的方法。分片方法的关键问题在于:如何确定轨迹片段的长度。如果轨迹片段太短,则无异于位置隐私保护,起不到轨迹隐私保护的作用;如果轨迹片段太长,则起不到划分的效果。轨迹划分的方法是将二维空间划分为大小相等的正方形"格",根据用户的隐私需求可将一个或多个"格"定义为一个"大格"。假如一条轨迹穿过不同的"大格","大格"的边界将这条轨迹分成若干个轨迹片段,然后再分别对处于不同"大格"的轨迹片段进行匿名。在划分交界处的位置隐私保护也是需要关注的问题,有的学者则提出在边界位置延时发布匿名区域的策略。

2) 基于历史轨迹的 k-匿名

多数匿名方法都是和当前时间段内的移动对象匿名,匿名是否成功很大程度上依赖于路网的稠密度。如果路网过于稀疏,容易造成匿名框过大,从而影响服务质量;若在服务时间内达不到用户设定的隐私级别,则会造成匿名失败。基于上述问题,有的研究者提出了用

历史数据和用户的运行轨迹匿名的方法。历史数据匿名技术采用中心服务器模式,客户端和位置服务器之间有一个可信的匿名服务器,且匿名服务器中含有存储历史轨迹数据的数据库。移动对象增量地向匿名服务器发送运行轨迹 $T_0=\{c_1,c_2,\cdots,c_n\}$,匿名服务器需要为 T_0 产生匿名区域的序列 $T=\{c_1,c_2,\cdots,c_n\}$,使 T 完全覆盖 T_0,且包含 $k-1$ 条历史轨迹。该方法通过为每一条历史轨迹建立基于格的索引来获取距离 T_0 最近的历史轨迹。在基于格的索引中,先使用四分树将二维空间划分为大小不等的“格”,为每个“格”维护一张表,表中存储了经过该“格”的轨迹 id 以及其他信息。通过该索引可以找到与 T_0 经过相同“格”的轨迹,并将这些轨迹存入集合 B 中,如果 B 中的轨迹数据不足 $k-1$ 个,则继续查找经过与 T_0 相邻的格的轨迹放入 B 中,直至 B 中含有至少 $k-1$ 条轨迹为止。由于 B 中的轨迹和 T_0 经过相同或相邻的“格”,距离 T_0 较近。形成轨迹 k-匿名的轨迹从集合 B 中选取。这样就完成了轨迹 k-匿名。

6.6.4 基于抑制法的轨迹隐私保护技术

抑制法是指有选择地发布原始数据,抑制某些数据项,即不发布某些数据项。如表 6-7 和表 6-8 所示展示了通过抑制法进行轨迹隐私保护的例子。表 6-7 中存储了坐标与语义位置之间的对应关系(该信息可以通过反向地址解析器和黄页相结合得到),假如攻击者获得该信息,就可以作为背景知识对发布的数据进行推理攻击。

表 6-7 位置信息表

位　　置	名　　称
(1,2)	体育馆
(2,7)	图书馆
(5,8)	网吧
(3,9)	酒店

表 6-8 用抑制法隐私保护的数据

MOB	t_1	t_2	t_3
O_1	—	(3,3)	(5,3)
O_2	(2,3)	—	(3,8)
O_3	(1,4)	(3,6)	—

表 6-8 是经过简单抑制之后发布的轨迹数据,可以看出,所有敏感位置信息都被限制发布,移动对象的隐私得到保护。

简单地说,抑制法包括两个重要原则:

(1) 抑制敏感/频繁访问的位置信息。

(2) 抑制增大整条轨迹披露风险的位置信息。

如何找到需要抑制的位置信息以降低披露风险且尽可能地提高数据的可用性是抑制法需要解决的关键问题。抑制法的研究者根据攻击者掌握移动对象的部分轨迹的情况,提出了抑制某些信息来保护移动用户轨迹隐私的方法。该方法要解决的问题是将轨迹数据库 D 转换为 D *,使得攻击者 A 不能以高于 P_{br} 的概率推导出轨迹上的位置属于某个移动对象。

假定轨迹 T 上的位置 p_j 来源于位置集合 P，不同的攻击者拥有不同的位置集合，攻击者 A 的位置集合表示为 PA，攻击者 A 掌握的轨迹片段表示为 TA。

因此，需要计算某个不属于 PA 的位置可能被 A 推导出其所有者的概率，如果这个概率大于 P_{br}，则 p_j 必须被抑制。使用抑制法进行隐私保护时，如果抑制的数据太多，势必会严重影响数据的可用性。

也有些研究者采用了另一种抑制法进行隐私保护。该方法根据某个区域访问对象的多少将地图上的区域分为敏感区域和非敏感区域，一旦移动对象进入敏感区域，将抑制或推迟其位置更新，以保护其轨迹隐私。对于非敏感区域，算法并不限制移动对象的位置更新。

抑制法简单有效，能处理攻击者持有部分轨迹数据的情况。在保证数据可用性的前提下，抑制法是一种效率较高的方法。然而，上面提到的方法仅适用于了解攻击者拥有某种特定背景知识的情形，当隐私保护方不能确切地知道攻击者的背景知识时，这种方法就不再适用了。

6.6.5　各类轨迹保护方法比较

以上对常用的 3 类轨迹隐私保护方法进行了介绍，本节对这 3 类方法进行比较，列举各类方法的主要优点、主要缺点以及代表技术，如表 6-9 所示。

表 6-9　各种隐私保护方法比较

方　法	主要优点	主要缺点	代表技术
假数据法	计算开销较小 比较容易实现	数据失真严重 算法移植性差	Dummy Path Protection
泛化法	算法移植性好 数据比较真实 比较容易实现	实现最优化轨迹 匿名开销较大； 有隐私泄露风险	(k,δ)-anonymit y Anonym ity-reconst ruction Split-generalization History data anonymity ExtremeUnion Symmetric Anonymization
抑制法	隐私保护度高 比较容易实现	数据失真严重	Suppression-based Location tracking

总的来说，这 3 类方法各有优缺点：假数据法计算开销小，实现简单，但是算法移植性较差、数据可用性/服务质量较差；而泛化法虽然算法移植性以及数据可用性/服务质量有较高的提升，但是实现代价也大大提高；抑制法实现简单且隐私保护度较高，然而数据失真严重。设计隐私保护方法时，要根据隐私保护的需求，并从攻击模型出发，选择合适的隐私保护算法。

6.7　本章小结

云计算是一种新兴的商业计算模型，它利用高速互联网的传输能力，将数据的处理过程从个人计算机或服务器转移到一个大型的计算中心，并将计算能力、存储能力当作服务来提

供,就如同电力、自来水一样按使用量进行计费。

云服务包括三种典型服务模式:基础设施即服务、平台即服务、软件即服务。

现有的标志性云平台包括 Google 云计算平台、IBM“蓝云”计算平台、Amazon 的弹性计算云。

云计算系统运用了许多技术,其中以编程模型、数据管理技术、数据存储技术、虚拟化技术、云计算平台管理技术最为关键。

云安全的几大核心问题包括身份与权限控制、Web 安全防护、虚拟化的安全、云安全服务。

云计算安全关键技术主要包括虚拟机安全技术、海量用户的身份认证、隐私保护与数据安全三个方面。

云计算技术是物联网涵盖的技术范畴之一。随着物联网的发展,未来物联网将势必产生海量数据,而传统的硬件架构服务器将很难满足数据管理和处理要求,将云计算运用到物联网的传输层和应用层,采用云计算的物联网,将会在很大程度上提高运作效率。

云计算与物联网的结合方式包括三种:单中心,多终端方式;多中心,大量终端方式;信息、应用分层处理,海量终端方式。

云计算技术应用于物联网可以解决如下问题:服务器节点不可信的问题,可以最大限度的降低服务器的出错概率;可以保障物联网在低的投入下,获得很好的经济收益;可以实现物联网由局域网到互联网的过程。

云计算与物联网结合面临的问题包括规模问题、安全问题、网络连接问题、标准化问题。

中间件是一种独立的系统软件或服务程序,分布式应用软件借助这种软件在不同的技术之间共享资源,中间件位于客户机服务器的操作系统之上,管理计算资源和网络通信。

中间件位于操作系统、网络和数据库的上层,应用程序的下层。中间件的核心作用是通过管理计算资源和网络通信,为各类分布式应用软件共享资源提供支撑。广义地看,中间件的总体作用是为处于自己上层的应用软件提供运行与开发的环境,帮助用户灵活地、高效地开发和集成复杂的应用软件。

基于目的和实现机制的不同,可以将中间件平台分为以下几类:远程过程调用(Remote Procedure Call Middleware, RPC)、面向消息的中间件(Message-Oriented Middleware, MOM)、对象请求代理(Object Request Broker, ORB)和事务处理监控(Transaction Processing Monitor, TPM)。

RFID 中间件是一种面向消息的中间件,信息以消息的形式从一个程序传送到另一个或多个程序。信息可以以异步的形式传送,所以传送者不必等待响应。

RFID 中间件可以从架构上分为以应用程序为中心和以软件架构为中心两类。

RFID 中间件的特点包括独立与架构、数据流、处理流和标准。

从发展趋势来分析,RFID 中间件可以分为三个发展阶段:应用程序中间件阶段、架构中间件阶段和解决方案中间件阶段。

在国际上,目前比较知名的 RFID 中间件厂商有 IBM、Oracle、Microsoft、SAP、Sun、Sybase、BEA 等国际知名企业。由于这些软件厂商自身都具有比较雄厚的技术储备,其开发的 RFID 中间件产品又经过多次的实验室、企业实地测试,RFID 中间件产品的稳定性、先进性、海量数据的处理能力都比较完善,已经得到了企业的普遍认可。

RFID技术进入中国的时间比较短，各方面的工作还处于起始阶段。虽然我国政府在国家十一五规划和863计划中，对RFID应用提供了政策、项目和资金的支持，并且RFID在国内的发展也较为迅速，但与国际先进技术的发展相比，在很多方面还存在明显的差距。

RFID中间件的设计，要遵循功能全面、容易设计、便于维护、具有良好的扩展性和可移植性的原则。设计RFID中间件至少要解决以下几个问题：屏蔽下层硬件，兼容不同的RFID读写器；对硬件设备进行统一管理；对数据流进行过滤和分组；数据接收和数据格式转换；中间件的安全问题；与企业应用程序的通信。

从中间件层的特点来分析，访问控制的实现依赖于引用监视器和访问策略的所在位置和实施。因此，可以根据安全逻辑的实现，将引用监视器的功能分成决策和执行两部分。

一般来说，中间件的设计应遵循整体的分层原则，中间件的系统结构自下向上可以分为硬件层、操作系统安全沙箱层、业务开发展和应用层。

自下向上的第一层，是包含各种不同设备的硬件、操作系统和驱动程序层。这一部分的差异较大，从低端的单片机到高端的DSP数字信号处理器或者PowerPC通信处理器都会出现在这一层。

自下向上的第二层，是运行于各种硬件之上的软件环境，这一部分的差异较硬件层小，通常由Linux和Windows CE等各种移动终端操作系统和驱动程序组成，其功能类似。

移植层用作屏蔽底层差异，实现中间件的统一实施接口，同时也是平台的主要功能的体现接口。

中间件的关键模块是中间件安全沙箱层，其内部包含多种执行模块，如RFID模块、通信模块和硬件控制模块等，所有的模块统一位于一个安全沙箱层中。该安全沙箱可以保证通信协议和远程控制对本地资源的安全访问。

中间件的最上层是业务开发层，该层提供给本地或远程应用程序调用，以实现相应的业务功能。其接口设计一般包含物联网设备的控制，信息读写、通信、显示、授权认证等通用接口，并将这些模块的实现映射到安全沙箱中解析或执行。

数据信息安全是指数据信息的硬件、软件及数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，数据信息服务不中断。数据安全主要是指数据信息的完整性、可用性、保密性和可靠性。

数据保护既是保证数据可用性，同样是保证业务连续性。数据保护的核心是建立和使用数据副本的技术。数据保护技术涉及主要有备份、复制技术、镜像技术、快照技术和连续数据保护技术等。

为了适应和满足数据共享的环境和要求，DBMS要保证整个系统的正常运转，防止数据意外丢失和不一致数据的产生，以及当数据库遭受破坏后能迅速地恢复正常，这就是数据库的保护。数据库保护又叫做数据库控制，是通过四方面实现的，即安全性控制，完整性控制，并发性控制和数据恢复。

数据容灾(Disaster Tolerance)，就是在灾难发生时，在保证应用系统的数据尽量少丢失的情况下，维持系统业务的连续运行。衡量容灾系统有三个主要指标：RPO、RTO和备份窗口(backup window)。一个容灾系统中实现数据容灾和应用容灾采取不同的实现技术。数据容灾的技术包括数据备份技术、数据复制技术和数据管理技术等，而应用容灾包括灾难检测技术、系统迁移技术和系统恢复技术等。

简单地说，隐私就是个人、机构等实体不愿意被外部世界知晓的信息。在具体应用中，隐私即为数据所有者不愿意被披露的敏感信息，包括敏感数据以及数据所表征的特性。

隐私可以分为两类：个人隐私、共同隐私。

数据隐私保护的效果，是由通过攻击者披露隐私的多少来侧面反映的。现有的隐私度量都可以统一用“披露风险”(Disclosure Risk)来描述。披露风险表示攻击者根据所发布的数据和其他背景知识(Background Knowledge)，可能披露隐私的概率。

数据隐私保护技术分为三类：基于数据失真(Distorting)的技术、基于数据加密的技术和基于限制发布的技术。

位置隐私保护不是指要保护用户的个人信息不被他人使用，而是指用户对个人的位置信息进行有效控制的权利。位置信息是一种特殊的个人隐私信息，对其进行保护就是要给予所涉及的个人决定和控制自己所处位置的信息何时、如何及在何种程度上被他人获知的权利。

轨迹隐私是一种特殊的个人隐私，它是指个人运行轨迹本身含有的敏感信息(如访问过的敏感位置)，或者由运行轨迹推导出的其他个人信息(如家庭住址、工作地点、生活习惯、健康状况等)。因此，轨迹隐私保护即要保证轨迹本身的敏感信息不泄露，又要防止攻击者通过轨迹推导出其他的个人信息。

轨迹隐私保护技术大致可以分为以下 3 类：基于假数据的轨迹隐私保护技术、基于泛化法的轨迹隐私保护技术、基于抑制法的轨迹隐私保护技术。

复习思考题

1. 简述云计算的基本概念。
2. 请列出有代表性的云计算平台。
3. 请列出三种典型的云服务模式，并分别说明每一种服务模式的内容。
4. 云计算的核心技术有哪些？
5. 与传统安全相比，云计算安全具有哪些新的特征？
6. 云安全的核心问题有哪些？
7. 请列举几个最严重的云计算安全威胁的事件。
8. 云计算安全关键技术包括哪些？
9. 虚拟机中的安全问题是什么？
10. 虚拟机中采用的防护方法有哪些？
11. 云计算环境下的用户隐私保护和数据安全主要包括哪些内容？
12. 云计算与物联网有哪些关系？
13. 云计算与物联网的结合方式是什么？
14. 云计算与物联网结合面临哪些问题？
15. 什么是中间件？请给出 IDC 对中间件的定义。
16. 中间件的产生与迅速发展的原因是什么？
17. 基于目的和实现机制的不同，可以将中间件平台分为哪几类？
18. RFID 中间件的发展可以分为哪些阶段？

19. 请简要说明在国际上 RFID 中间件的发展现状。
20. 设计 RFID 中间件至少要解决哪些问题?
21. 在通用的中间件安全模型中,可以将引用监视器的功能分成哪些部分?
22. 请遵循整体的分层设计原则,画图描述中间件的框架。
23. 什么是沙箱技术?
24. 数据安全的含义是什么? 数据安全要素是哪些?
25. 用于数据安全的技术主要有哪些?
26. 数据保护含义是什么? 衡量数据保护的两个重要标准是什么?
27. 数据保护技术实现分几个层次? 各层次使用的技术是什么?
28. 对数据库的保护是通过哪几个方面实现的?
29. 数据库怎样进行并发控制? 怎样避免数据库操作的死锁?
30. 简述数据库的恢复方法。
31. 数据容灾的含义是什么? 衡量数据容灾的主要指标是什么?
32. 数据容灾的主要技术有哪些?
33. 什么是隐私? 隐私保护技术分为哪些类别?
34. 什么是位置隐私保护? 如何实现位置隐私保护?
35. 什么是轨迹隐私保护?
36. 如何实现基于假数据的轨迹隐私保护技术?
37. 如何实现基于泛化法的轨迹隐私保护技术?
38. 如何实现基于抑制法的轨迹隐私保护技术?

第7章 物联网安全管理

7.1 物联网安全管理概述

物联网安全管理是指导和控制企业的关于信息安全风险的相互协调活动。关于信息安全风险的指导和控制活动,通常包括制订信息安全方针、风险评估、控制目标与方式选择、风险控制、安全保证等。而要对企业的信息安全进行高效、动态的管理,就必须依据信息安全管理模型和信息安全管理标准构建企业的信息安全管理体系。

信息安全管理体系(Information Security Management System,ISMS)是1998年前后从英国发展起来的信息安全领域中的一个新概念,是管理体系(Management System,MS)思想和方法在信息安全领域的应用。近年来,伴随着信息安全管理体系国际标准的制订,ISMS迅速被全球接受和认可,成为世界各国、各种类型、各种规模的企业或组织解决信息安全问题的一个有效方法。ISMS认证随之成为企业或组织向社会及其相关方证明其信息安全水平和能力的一种有效途径。

信息安全管理体系是企业按照信息安全管理体系相关标准的要求,制订信息安全管理方针和策略,采用风险管理的方法进行信息安全管理计划、实施、评审检查、改进的信息安全管理执行的工作体系。信息安全管理体系是按照ISO/IEC 27001标准《信息技术-安全技术-信息安全管理体系要求》的要求建立的,ISO/IEC 27001标准是由BS 7799-2标准发展而来的。

信息安全管理体系要求企业通过确定信息安全管理体系范围、制订信息安全方针、明确管理职责、以风险评估为基础选择控制目标与控制方式等活动建立信息安全管理体系;体系一旦建立,企业应按体系规定的要求进行运作,保持体系运作的有效性;信息安全管理体系应形成一定的文件,即企业应建立并保持一个文件化的信息安全管理体系,其中应阐述被保护的资产、企业风险管理的方法、控制目标及控制方式和需要的保证程度。

7.2 信息安全标准化组织

7.2.1 国际信息安全标准化组织

国际上信息安全标准化工作起源于20世纪70年代中期,在20世纪80年代发展迅速,在20世纪90年代引起了世界各国的普遍关注。

国际标准化组织(ISO)和国际电工委员会(IEC)是世界范围的标准化组织,由各个国家和地区的成员组成,各国的相关标准化组织都是其成员,他们通过各技术委员会,参与相关标准的制订。

为了更好地协作和共同规范信息技术领域,国际标准化组织(ISO)和国际电工委员会(IEC)成立了联合技术委员会,即 ISO/IEC JTC1,负责信息技术领域的标准化工作。其中的子委员会 27 专门负责 IT 安全技术领域的标准化工作。

目前,国际上共有近 300 个国际和区域性组织制订标准或技术规则。总的来说,与信息安全标准化相关的国际信息安全标准化组织主要是以下 4 个国际组织:

1. 国际标准化组织

国际标准化组织(International Organization for Standardization,ISO)是一个全球性的非政府组织,是国际标准化领域中一个十分重要的组织。ISO 一词来源于希腊语"ISOS",即"EQUAL"——平等之意。ISO 国际标准组织成立于 1946 年,中国是 ISO 的正式成员,代表中国参加 ISO 的国家机构是中国国家技术监督局(CSBTS)。

ISO 负责目前绝大部分领域(包括军工、石油、船舶等垄断行业)的标准化活动。截至 2013 年 5 月,ISO 共有 163 个成员国。ISO 的最高权利机构是每年一次的"全体大会",其日常办事机构是中央秘书处,设在瑞士日内瓦。中央秘书处现有 170 名职员,由秘书长领导。ISO 的宗旨是"在世界上促进标准化及其相关活动的发展,以便于商品和服务的国际交换,在智力、科学、技术和经济领域开展合作。"ISO 通过它的 2671 个技术机构开展技术活动,其中技术委员会(SC)共 611 个,工作组(WG)2022 个,特别工作组 38 个。中国于 1978 年加入 ISO,在 2008 年 10 月的第 31 届国际化标准组织大会上,中国正式成为 ISO 的常任理事国。

国际标准化组织总部设于瑞士日内瓦,该组织自我定义为非政府组织,官方语言是英语、法语和俄语。参加者包括各会员国的国家标准机构和主要公司。它是世界上最大的非政府性标准化专门机构,是国际标准化领域中一个十分重要的组织。

国际标准化组织的信息技术标准化委员会(ISO/IEC JTC1)所属安全技术分委员会(SC 27)的前身,是数据加密分技术委员会(SC 20),主要从事信息技术安全的一般方法和技术的标准化工作。

而 ISO/TC68 负责与银行业务应用范围内有关信息安全标准的制订,它主要制订行业应用标准,在组织上和标准之间与 SC 27 有着密切的联系。ISO/IEC JTC1 负责制订的标准主要是开放系统互连、密钥管理、数字签名、安全评估等方面的内容。

2. 国际电工委员会

国际电工委员会(IEC)成立于 1906 年,至 2015 年已有 109 年的历史。它是世界上成立最早的国际性电工标准化机构,负责有关电气工程和电子工程领域中的国际标准化工作。国际电工委员会的总部最初位于伦敦,1948 年搬到了位于日内瓦的现总部处。在 1887—1900 年召开的 6 次国际电工会议上,与会专家一致认为有必要建立一个永久性的国际电工标准化机构,以解决用电安全和电工产品标准化问题。1904 年在美国圣路易召开的国际电工会议上通过了关于建立永久性机构的决议。1906 年 6 月,13 个国家的代表集会伦敦,起草了 IEC 章程和议事规则,正式成立了国际电工委员会。1947 年作为一个电工部门并入国

际标准化组织(ISO),1976年又从ISO中分立出来。宗旨是促进电工、电子和相关技术领域有关电工标准化等所有问题上(如标准的合格评定)的国际合作。

在信息安全标准化方面,除了与ISO联合成立了JTC1属的分委员会外,它还在电信、电子系统、信息技术和电磁兼容等方面成立了技术委员会,并为信息技术设备安全(IEC 60950)等制订相关国际标准。

3. 国际电信联盟

国际电信联盟(International Telecommunication Union,ITU)简称为国际电联,是联合国的一个重要专门机构,也是联合国机构中历史最长的一个国际组织。

国际电联是主管信息通信技术事务的联合国机构,负责分配和管理全球无线电频谱与卫星轨道资源,制订全球电信标准,向发展中国家提供电信援助,促进全球电信发展。

作为世界范围内联系各国政府和私营部门的纽带,国际电联通过其麾下的无线电通信、标准化部门开展活动,而且是信息社会世界高峰会议的主办机构。

国际电联总部设于瑞士日内瓦,其成员包括193个成员国和700多个部门成员及部门准成员和学术成员。每年的5月17日是世界电信日(World Telecommunication Day)。

国际电信联盟所属的SG17组主要负责研究通信系统安全标准。SG17组主要研究的内容包括:通信安全项目、安全架构和框架、计算安全、安全管理、用于安全的生物测定、安全通信服务。此外,SG16和下一代网络核心组也在通信安全、H323网络安全、下一代网络安全等标准方面开展了研究工作。

4. Internet 工程任务组

互联网工程任务组(The Internet Engineering Task Force,IETF)成立于1985年底,是全球互联网最具权威的技术标准化组织,主要任务是负责互联网相关技术规范的研发和制订,当前绝大多数国际互联网技术标准都出自IETF。

IETF是一个由为互联网技术工程及发展做出贡献的专家自发参与和管理的国际民间机构。它汇集了与互联网架构演化和互联网稳定运作等业务相关的网络设计者、运营者和研究人员,并向所有对该行业感兴趣的人士开放。

IETF的主要任务是负责互联网相关技术标准的研发和制订,是国际互联网业界具有一定权威的网络相关技术研究团体。

互联网工程任务组制订标准的具体工作由各个工作组承担,工作组分成8个领域,涉及Internet路由、传输、应用领域等等,包含在RFC系列之中的IKE和IPSec,还有电子邮件,网络认证和密码标准,此外,也包括了TLS标准和其他的安全协议标准。

7.2.2 中国信息安全标准化组织

中国政府主管部门以及各行各业已经认识到了信息安全的重要性。政府部门已经出台了一系列相关的政策和法规,直接牵引、推进信息安全的应用和发展。

由中国政府主导的各大信息系统工程和信息化程度要求非常高的相关行业,也开始出台信息安全技术产品的应用标准和规范。

物联网标准的划分应该是分层次的,如传感器的、应用的、传输的等,或者细化为芯片、

电路、通信接口、路由等层次，而目前我国在物联网标准方面制订的主要是在传感器上的标准，是传感网络路由层面的专利。

目前，我国物联网技术的研究水平已位于国际前列，与德国、美国、日本等国一起，成为国际物联网标准制订的主要国家，逐步成为全球物联网产业链中重要的一环。

1. 信息安全标准化组织的发展

目前，根据中国国务院授权，在国家质量监督检验检疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，下设有255个专业技术委员会。

中国标准化工作实行统一管理与分工负责相结合的管理体制，分工管理本行政区域内、本部门、本行业的标准化工作。

2. 信息安全标准化组织

中国的信息安全标准化组织主要包括以下几个：

1）中国信息安全标准化技术委员会

成立于1984年的中国信息技术安全标准化技术委员会(CITS)，在国家标准化管理委员会和信息产业部的共同领导下，负责全国信息技术领域以及与ISO/IEC JTC1相对应的标准化工作，下设24个分技术委员会和特别工作组，是目前国内最大的标准化技术委员会。它是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。

2）公安部信息系统安全标准化技术委员会

为了适应我国信息化进程的飞速发展，保障我国信息系统和信息网络的安全，促进信息安全产业的形成和发展，满足公安机关对信息系统实施安全保护与监察的工作需要，更好地开展信息系统安全技术领域的标准化工作，公安部信息系统安全标准化技术委员会于1999年3月经公安部科技局批准正式成立。主要任务是在公安部的领导下，负责规划和制订我国信息安全标准和技术规范，监督技术标准的实施。

3）中国通信标准化协会网络与信息安全技术工作委员会

中国通信标准化协会网络与信息安全技术工作委员会(CCSA)成立于2002年12月，其组织结构如图7-1所示。

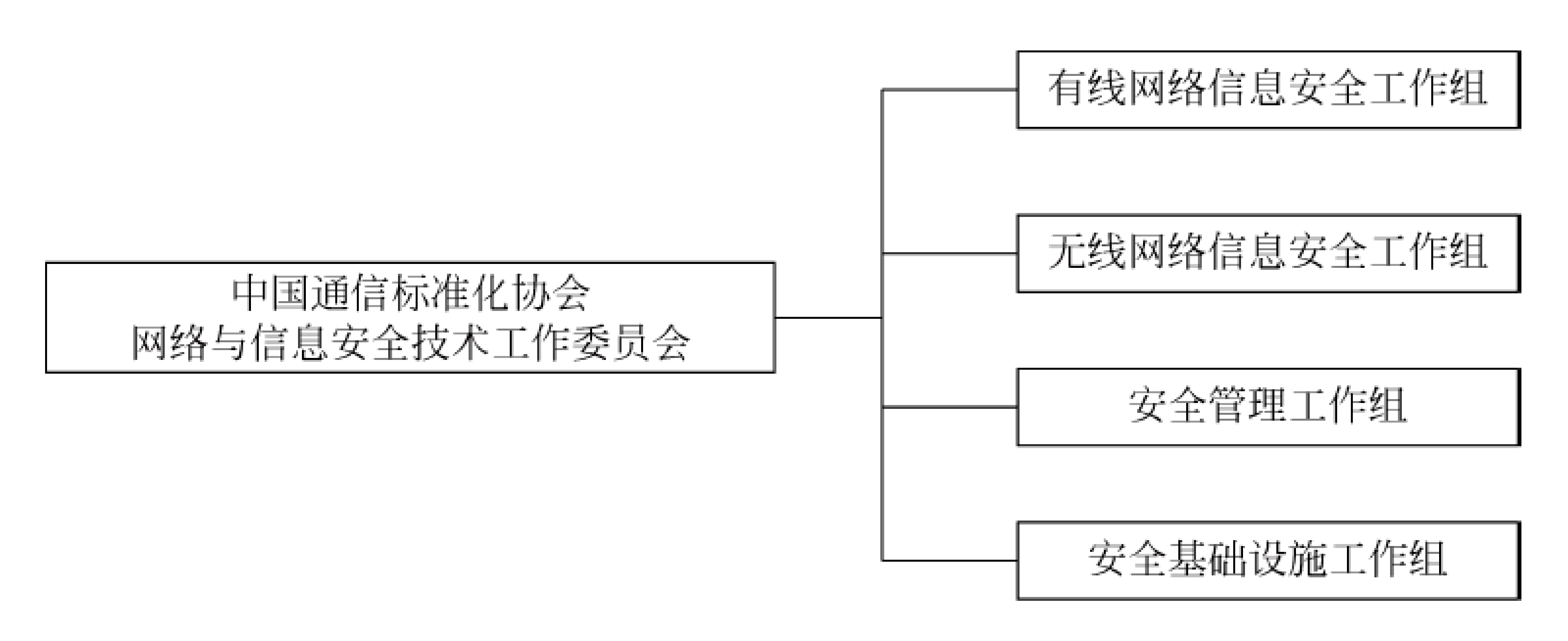


图7-1　网络与信息安全技术工作委员会

CCSA下设了有线网络信息安全、无线网络信息安全、安全管理和安全基础设施4个工作组。其中，有线网络信息安全工作组主要负责研究包括有线网络中电话网、互联网、传输

网、接入网等在内所有电信网络相关的安全标准；无线网络信息安全工作组主要负责研究无线网络中接入、核心网、业务等相关的安全标准；安全管理工作组主要负责研究有线网络和无线网络相关的管理标准；安全基础设施工作组主要负责研究网络安全基础设施相关的标准。

4）中国电子标签国家标准工作组

2005 年 12 月，中国电子标签标准工作组在北京正式宣布成立。该工作组的任务是联合社会各方面力量，开展电子标签标准体系的研究，并以企业为主体进行标准的预先研究和制/修订工作。中国电子标签国家标准工作组的组织结构如图 7-2 所示。



图 7-2　中国电子标签国家标准工作组的组织结构

5）中国传感器网络标准工作组

2009 年 9 月，中国传感器网络标准工作组成立大会暨“感知中国”高峰论坛在北京举行。

中国传感器网络标准工作组是由国家标准化管理委员会批准筹建，全国信息技术标准化技术委员会批准成立并领导，从事传感器网络（简称传感网）标准化工作的全国性技术组织。

6）中国泛在网技术工作委员会

2010 年 2 月，中国通信标准化协会（CCSA）泛在网技术工作委员会（TC10）成立大会暨第一次全会在北京召开。

TC10 的成立，标志着 CCSA 今后泛在网技术与标准化的研究将更加专业化、系统化、深入化，必将进一步促进电信运营商在泛在网领域进行积极的探索和有益的实践，不断优化设备制造商的技术研发方案，推动泛在网产业健康快速发展。

7）中国物联网标准联合工作组

2010 年 6 月，在国家标准化管理委员会、工业和信息化部等相关部委的共同领导和直接指导下，由全国工业过程测量和控制标准化技术委员会、全国智能建筑及居住区数字化标

准化技术委员会、全国智能运输系统标准化技术委员会等19家现有标准化组织联合倡导并发起成立物联网标准联合工作组。

3. 中国信息安全标准体系研究特点

(1) 基于信息内容的过滤和管制技术将越来越受关注。

(2) 防范和治理垃圾信息成为网络安全研究重要内容。

(3) 网络与信息安全研究重点将逐渐从设备层面向网络层面转移。

(4) 业务安全越来越成为运营商研究重点。

(5) 认证技术将研究和梳理,生物鉴别成为重要内容。

(6) 网络建设将重视信任体系的建设。

(7) 互联网安全将进一步研究,其成果将适用于下一代网以及3G核心网。

(8) 网络上信息安全将划分责权,网络侧重负责部分私密性(隔离)和完整性,机密性和不可否认性由端到端保障。

(9) 安全管理中的安全风险评估将成为安全研究重要内容。

4. 中国信息安全标准化的发展趋势

(1) 走国际化合作之路。

(2) 走商业化发展之路。

(3) 明确研究方向。

7.3 信息安全管理模型

信息安全管理模型是对信息安全管理的一个抽象化描述。它是企业建立安全管理体系的基础。目前,在对安全理论、安全技术和安全标准研究的基础上,不同的组织都提出了相应的信息安全管理模型。这些模型的侧重点各有不同,信息安全的管理方式也不同。以下着重介绍OSI安全体系结构模型,其他信息安全管理模型则作简要的介绍。

7.3.1 OSI安全体系结构模型

OSI安全体系结构模型是根据OSI七层协议模型建立的。也就是说,OSI安全体系结构与OSI网络模型的七层是相对应的。在不同的层次上都有不同的安全技术。OSI安全体系结构模型如图7-3所示。

在OSI安全体系结构模型中,每一层采用的安全技术如下。

1. 数据链路层

在数据链路层,OSI安全体系结构模型采用点到点通道协议(PPTP)和第二层通道协议(L2TP)。

点到点通道协议PPTP,英文全称为Point to Point Tunneling Protocol。它是一种支持多协议虚拟专用网的新型技术,可以使远程用户通过Internet安全地访问企业网。这就是

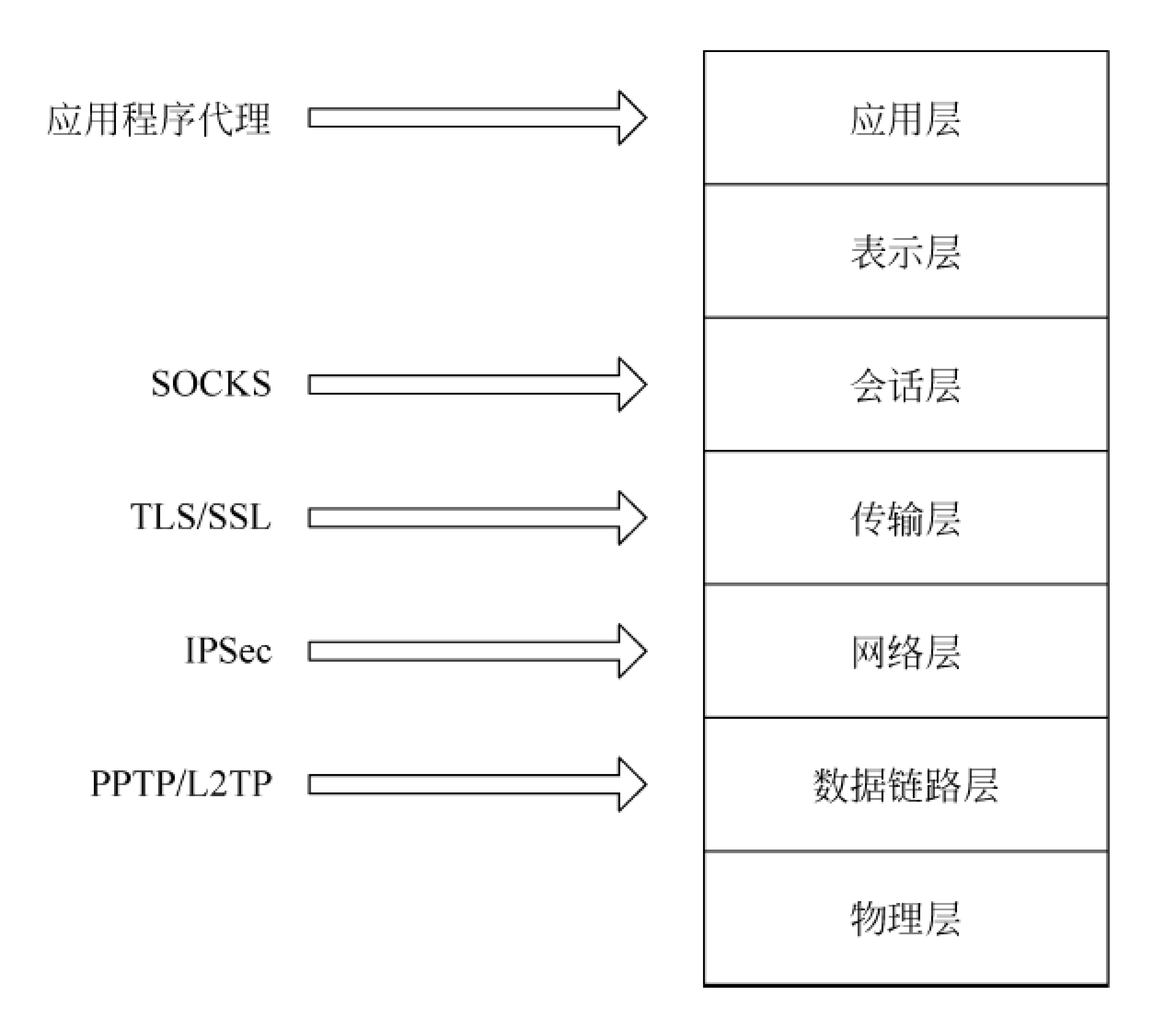


图 7-3 OSI 安全体系结构模型

通常所用的 VPN 技术。使用 PPTP 协议，远程用户可以通过任意一款网络操作系统连接到 Internet，再通过公网连接到企业网络。即通过 PPTP 协议在所用的信道上建立了一个简单的加密隧道。

基于 PPTP 协议的 VPN 企业虚拟专用网如图 7-4 所示。

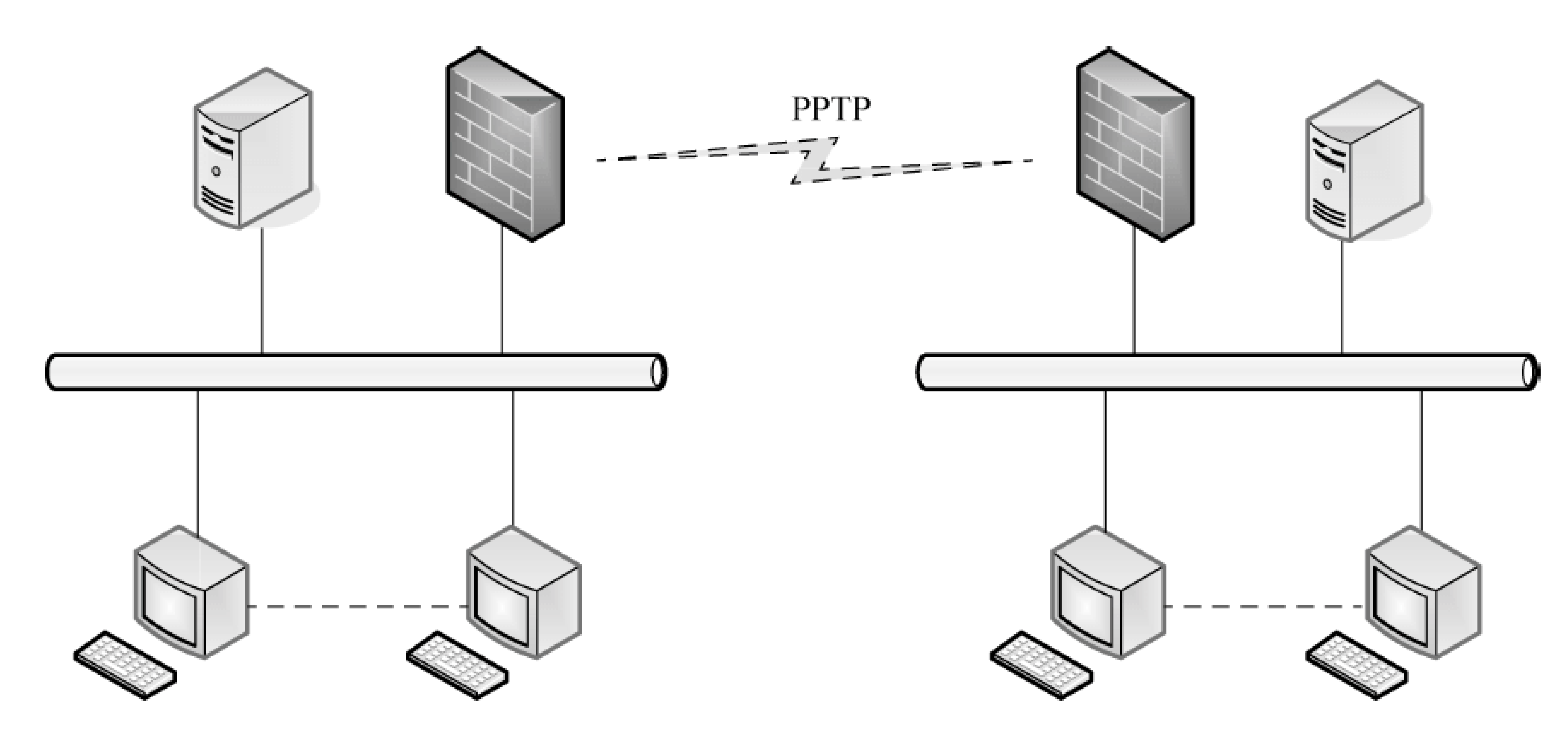


图 7-4 基于 PPTP 的 VPN 企业虚拟专用网

第二层通道协议（L2TP）是 Cisco 公司提出的把 L2F 与 PPTP 相结合的一个协议。L2TP 有一部分采用的是 PPTP 协议，比如同样可以对网络数据流进行加密。不过也有不同之处，比如 PPTP 要求网络为 IP 网络，L2TP 要求面向数据包的点对点连接；PPTP 使用单一隧道，L2TP 使用多隧道；L2TP 提供包头压缩、隧道验证，而 PPTP 不支持。

2. 网络层

在网络层，OSI 安全体系结构模型采用 IP 安全协议（IPSec）。

早在 IPv4 的最初设计时，仅仅考虑了信息资源的共享，并没有过多地考虑到网络安全

问题，因此无法从根本上防止网络层攻击。在现有的 IPv4 上应用 IPSec 可以加强其安全性，IPSec 在网络层提供了 IP 报文的机密性、完整性、IP 报文源地址认证以及抗伪地址的攻击能力。IPSec 可以保护在所有支持 IP 的传输介质上的通信，保护所有运行于网络层上的所有协议在主机间进行安全传输。IPSec 网关可以安装在需要安全保护的任何地方，如路由器、防火墙、应用服务器或客户机等。IPSec 协议的数据封装格式如图 7-5 所示。

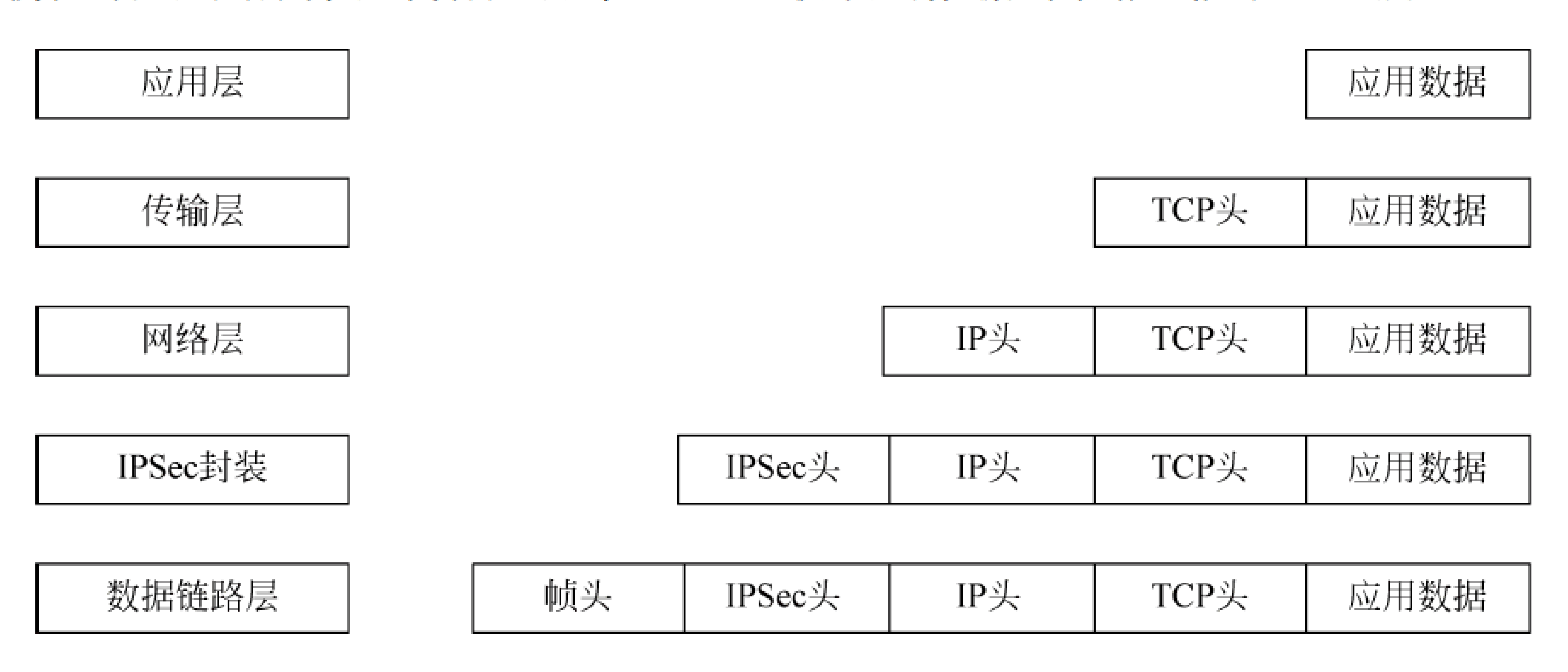


图 7-5　IPSec 协议的数据封装格式

IPSec 协议主要由三个部分组成：

(1) AH(Authentication Header)认证报头，提供对报文完整性的报文的源地址进行认证。

(2) ESP(Encapsulating Security Payload)封装安全载荷，提供对报文内容的加密和认证功能。

(3) IKE(Internet Key Exchange)Internet 密钥交换，协商信源和信宿节点间保护 IP 报文的 AH 和 ESP 的相关参数，如加密、认证的算法和密钥、密钥的生存时间等。AH 和 ESP 是网络层协议，IKE 是应用层协议。一般情况下，IPSec 仅指网络层协议 AH 和 ESP。由于 IPSec 服务是在网络层提供的，任何上层协议都可以使用此服务。

3. 传输层

在传输层，OSI 安全体系结构模型采用安全套接层协议(SSL)和传输层安全协议(TLS)。

安全套接层(Secure Sockets Layer，SSL)是美国网景公司(Netscape)在推出 Web 浏览器首版的同时，提出的加密协议。SSL 位于传输层上，其结构如图 7-6 所示。

SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。可在服务器和客户机两端同时实现支持，目前已成为互联网上保密通信的工业标准，现行 Web 浏览器普遍将 Http 和 SSL 相结合，从而实现安全通信。SSL 协议的优势在于它是与应用层协议独立无关的。高层的应用层协议(例如：Http、FTP、Telnet 等等)能透明地建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

传输层安全协议(Transport Layer Security，TLS)是确保互联网上通信应用和其用户

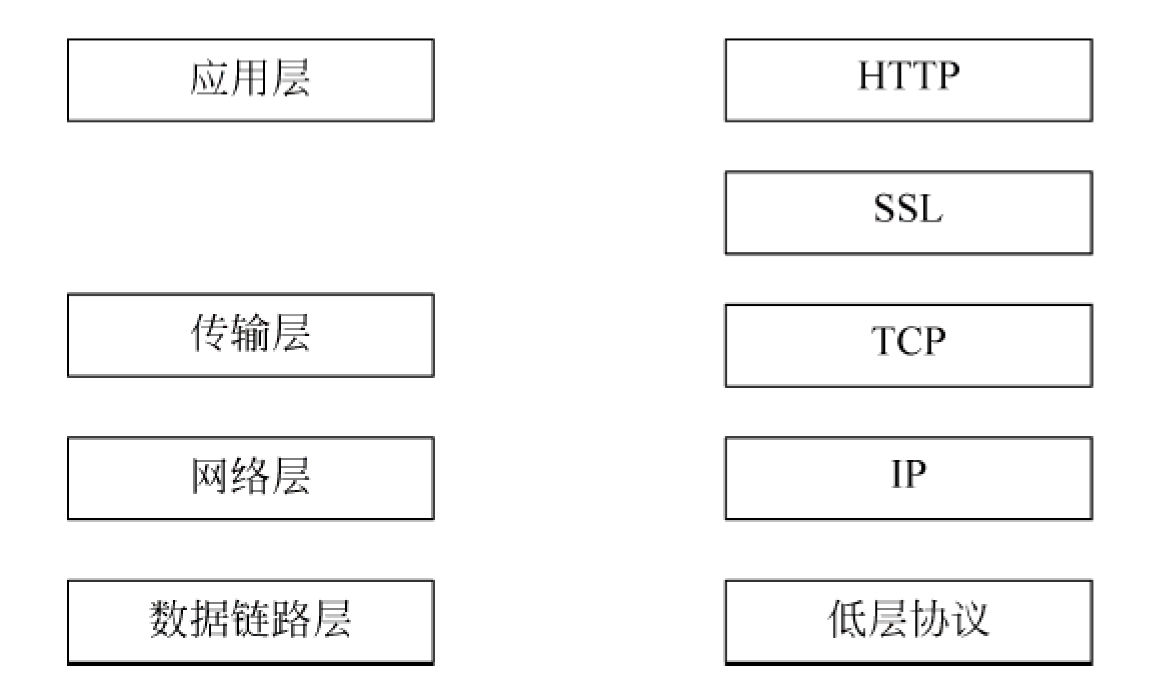


图 7-6　SSL 安全套接层协议结构图

隐私的协议。当服务器和客户机进行通信，TLS 确保没有第三方能窃听或盗取信息。TLS 是安全套接层（SSL）的后继协议。TLS 由两层构成：TLS 记录协议和 TLS 握手协议。TLS 记录协议使用机密方法，如数据加密标准（DES），来保证连接安全。TLS 记录协议也可以不使用加密技术。TLS 握手协议使服务器和客户端在数据交换之前进行相互鉴定，并协商加密算法和密钥。TLS 利用密钥算法在互联网上提供端点身份认证与通信保密，其基础是公钥基础设施（Public Key Infrastructure，PKI）。不过在实现的典型例子中，只有网络服务器被可靠身份验证，而其客户端则不一定。这是因为公钥基础设施普遍商业运营，电子签名证书相当昂贵，普通大众很难买得起证书。协议的设计在某种程度上能够使主从式架构应用程序通信本身预防窃听、干扰（Tampering）和消息伪造。

4. 会话层

在会话层，OSI 安全体系结构模型采用 SOCKS 代理技术。

SOCKS 是一种网络传输协议，主要用于客户端与外网服务器之间通信的中间传递。SOCKS 是 SOCKetS 的缩写。

当防火墙后的客户端要访问外部的服务器时，就跟 SOCKS 代理服务器连接。这个代理服务器控制客户端访问外网的资格，允许的话，就将客户端的请求发往外部的服务器。这个协议最初由 Devid Koblas 开发，而后由 NEC 的 Ying-Da Lee 将其扩展到版本 4。最新协议是版本 5，与前一版本相比，增加支持 UDP、验证以及 IPv6。根据 OSI 模型，SOCKS 是位于应用层与传输层之间的中间层。

5. 应用层

在应用层，OSI 安全体系结构模型采用应用程序代理技术。

应用程序代理工作在应用层之上，位于客户端与服务器之间，完全阻挡了二者间的数据交流。从客户端来看，代理服务器相当于一台真正的服务器；而从服务器来看，代理服务器又是一台真正的客户机。当客户端需要使用服务器上的数据时，首先将数据请求发给代理服务器，代理服务器再根据这一请求向服务器索取数据，然后再由代理服务器将数据传输给客户端。由于外部系统与内部服务器之间没有直接的数据通道，外部的恶意侵害也就很难伤害到企业内部网络系统。并对应用层以下的数据透明。应用层代理服务器用于支持代理的应用层协议，如：HTTP、HTTPS、FTP、TELNET 等。由于这些协议支持代理，所以只

要在客户端的浏览器或其他应用软件中设置“代理服务器”项，设置好代理服务器的地址，客户端的所有请求将自动转发到代理服务器中。然后由代理服务器处理或转发该请求。

7.3.2 P2DR 信息安全模型

P2DR 模型是美国 ISS 公司提出的动态网络安全体系模型，也是动态安全模型的雏形。P2DR 模型包括四个主要部分：Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）。P2DR 模型的结构如图 7-7 所示。

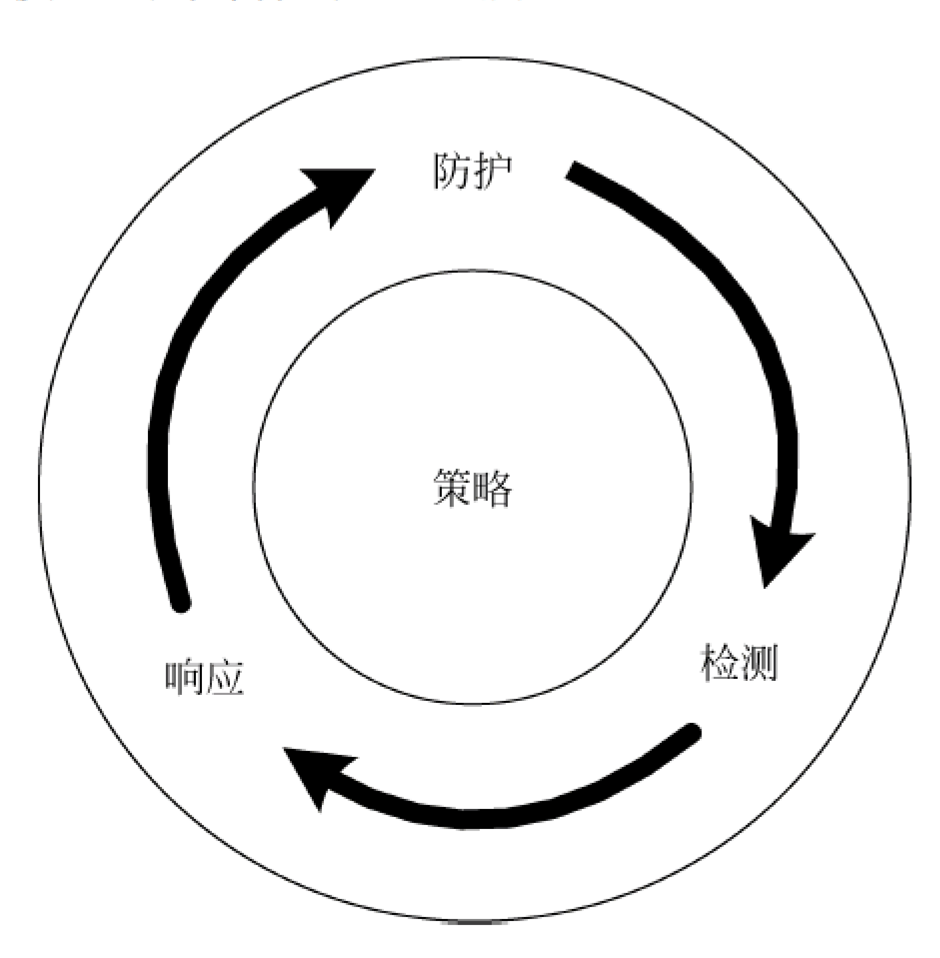


图 7-7 P2DR 信息安全模型

1. 策略

策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略 2 个部分。

2. 防护

防护是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

3. 检测

当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。检测是动态响应的依据。

4. 响应

系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操

作系统身份认证、加密等)的同时,利用检测工具(如漏洞评估、入侵检测等)了解和评估系统的安全状态,通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环,在安全策略的指导下保证信息系统的安全。

P2DR 模型的基本原理是,认为信息安全相关的所有活动,不管是攻击行为、防护行为、检测行为和响应行为等等都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系,当入侵者要发起攻击时,每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间 Pt;在入侵发生的同时,检测系统也在发挥作用,检测到入侵行为也要花费时间——检测时间 Dt;在检测到入侵后,系统会做出应有的响应动作,这也要花费时间——响应时间 Rt。

根据 P2DR 信息安全模型,我们可以通过一些典型的数学公式,量化地表达信息安全的要求:

公式 1:$Pt>Dt+Rt$

公式 2:如果 $Pt=0$,则 $Et=Dt+Rt$

Pt 代表系统为了保护安全目标设置各种保护后的防护时间;或者理解为在这样的保护方式下,黑客(入侵者)攻击安全目标所花费的时间。Dt 代表从入侵者开始发动入侵开始,系统能够检测到入侵行为所花费的时间。Rt 代表从发现入侵行为开始,系统能够做出足够的响应,将系统调整到正常状态的时间。那么,针对于需要保护的安全目标,如果上述数学公式满足防护时间大于检测时间加上响应时间,也就是在入侵者危害安全目标之前,入侵就能被检测到并及时处理。

公式 2 的前提是假设防护时间 Pt 为 0。Dt 代表从入侵者破坏了安全目标系统开始,系统能够检测到破坏行为所花费的时间。Rt 代表从发现遭到破坏开始,系统能够做出足够的响应,将系统调整到正常状态的时间。比如,对 Web Server 被破坏的页面进行恢复。那么,Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对于需要保护的安全目标,如果 Et 越小系统就越安全。

通过上面两个公式的描述,实际上给出了安全一个全新的定义:“及时的检测和响应就是安全”,“及时的检测和恢复就是安全”。而且,这样的定义为安全问题的解决给出了明确的方向:提高系统的防护时间 Pt,降低检测时间 Dt 和响应时间 Rt。

P2DR 模型存在一个明显的弱点,就是忽略了内在的变化因素,如人员的流动、人员的素质和策略贯彻的不稳定性。实际上,安全问题牵涉面广,除了涉及防护、检测和响应,系统本身安全的“免疫力”的增强、系统和整个网络的优化,以及人员这个在系统中最重要角色的素质提升,都是该安全系统没有考虑到的问题。

7.3.3 PDRR 信息安全模型

PDRR 信息安全模型的结构如图 7-8 所示。PDRR(Protection Detection Response Recovery)是一个比较成熟的网络安全模型,它可以用于信息安全管理。这个模型由防御、检测、响应、恢复组成一个动态的信息安全周期。安全策略共有四个部分,每一部分分别实现一定的安全功能。安全策略的第一部分是防御。根据系统已知的所有的安全问题做出防御措施,例如打补丁、访问控制、数据加密等。安全策略的第二部分是检测。假如攻击者穿

过了防御系统,检测系统就会检测出来。这一部分的功能是检测入侵者的身份,包括攻击源、系统受损状况等。安全策略的第三部分是响应。一旦检测出入侵,响应部分就立即作出反应,包括事件处理和其他业务。安全策略的最后一个部分是恢复。在入侵事件发生后,把系统恢复到原来的状态。

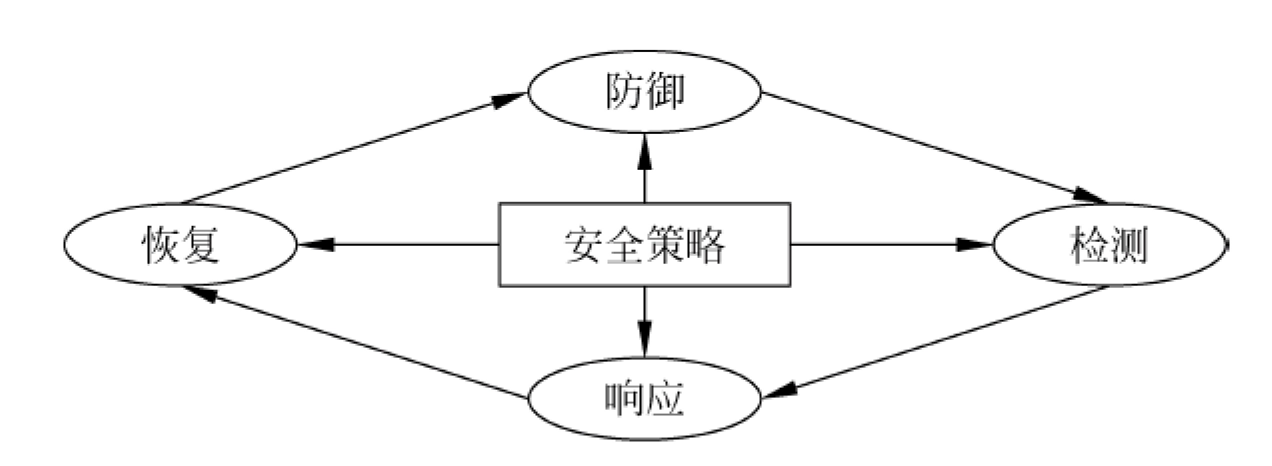


图 7-8 PDRR 信息安全模型

7.3.4 PDCA 持续改进模型

PDCA 持续改进模型的结构如图 7-9 所示。

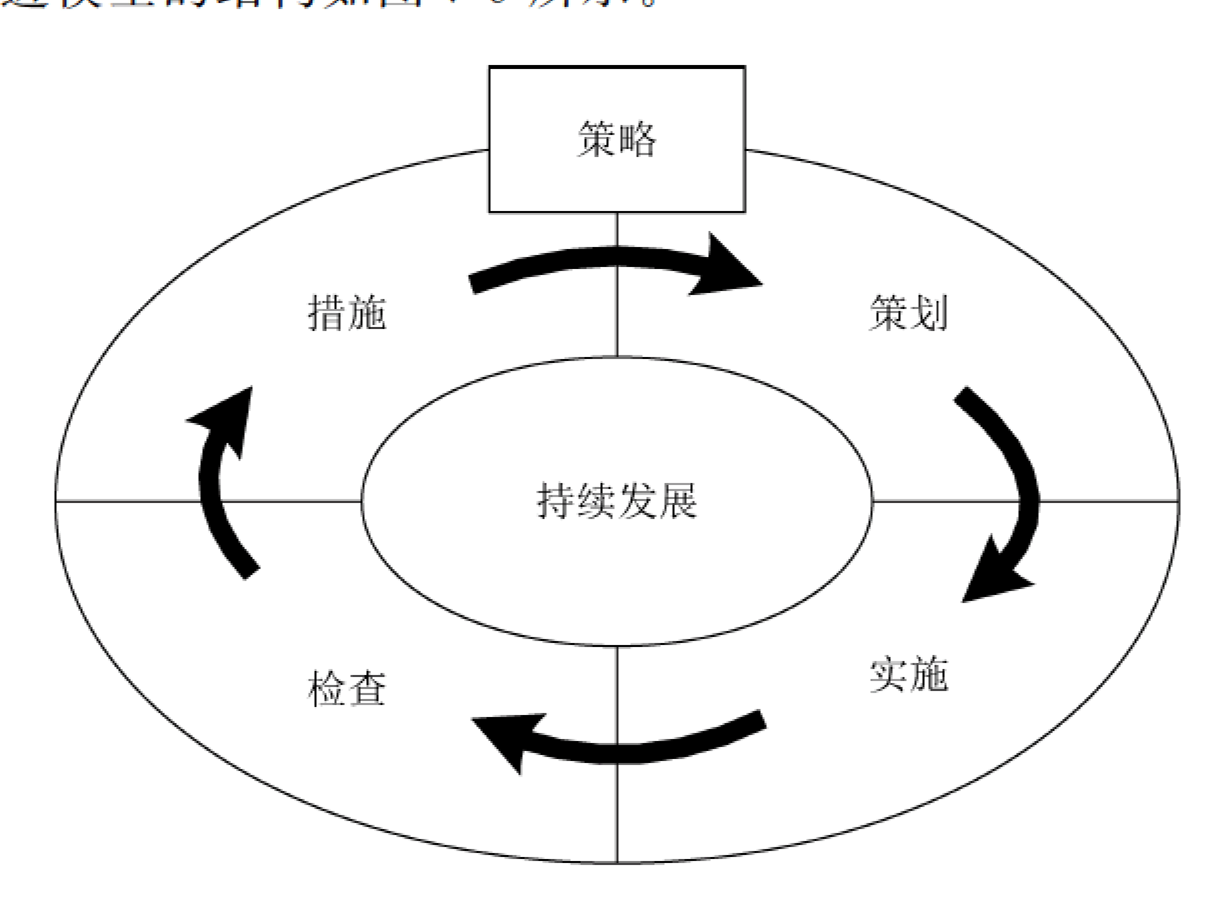


图 7-9 PDCA 持续改进模型

这个模型分为四个阶段。

(1) 策划阶段:根据企业的商务运作需求(包括顾客的信息安全需求)和有关法律法规的要求,确定安全管理的范围和策略,通过风险评估建立控制目标与方式,包括必要的过程与商务持续性计划;

(2) 实施阶段:即实施的过程,企业要根据策略、程序、规章等规定的要求,按照所选定的控制目标与方式进行信息安全控制;

(3) 检查阶段:根据策略、目标、安全标准及法律法规的要求,对安全管理过程和信息系统的安全进行监视与验证,并报告检查结果;

(4) 措施阶段:对策略适宜性进行评审和评估,评价信息安全管理系统的有效性,采取相应的措施,持续改进。

7.3.5 HTP信息安全模型

HTP信息安全模型的结构如图7-10所示。

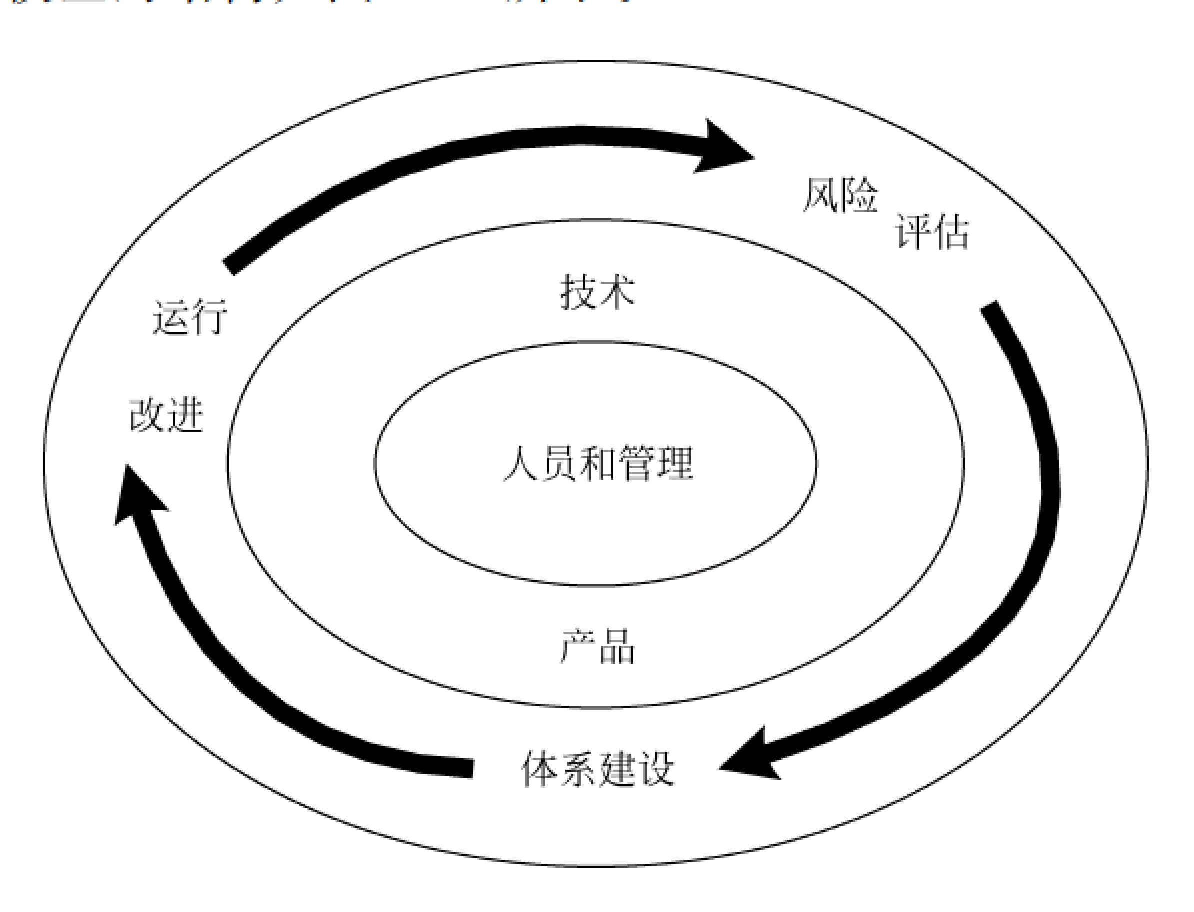


图7-10 HTP信息安全模型

HTP信息安全模型由三个部分组成：人员和管理(Human and Management)、技术和产品(Technology and Products)、流程和体系(Process and Framework)。

1. 人员和管理

从国家安全的角度分析，有法律、法规、政策问题；从企业安全的角度分析，有安全方针政策程序、安全管理、安全教育与培训、组织文化、应急计划和持续性管理等问题；从个人安全的角度分析，有职业要求、个人隐私、行为学、心理学等问题。人是信息安全最活跃的因素，人的行为是信息安全保障的重要方面。

2. 技术和产品

企业可以依据“适度防范”的原则综合采用商用密码、防火墙、防病毒、身份识别、网络隔离、可信服务、安全服务、备份恢复、PKI服务、取证、网络入侵陷阱、主动反击等多种技术和产品来保护信息系统安全。

3. 流程和体系

企业应当遵循国内外相关的信息安全标准与最佳实践过程，满足信息安全的各个层面的实际需求。在风险分析的基础上，引入恰当的控制措施，建立合理的安全管理体系，从而保证企业赖以生存的信息资产的安全性、完整性和可用性。

7.4 信息安全管理标准

2000年12月，国际标准化组织ISO正式发布了有关信息安全的国际标准《国际信息安全管理标准体系》(ISO 17799)，这个标准包括信息系统安全管理和安全认证两大部分，是参

照英国国家标准 BS 7799 发展而来的。它是一个详细的信息管理安全标准，包括安全内容的所有准则，由两大部分组成，每一部分都覆盖了不同的主题和区域。

7.4.1　英国 BS 7799 标准产生的背景及其产生

由英国标准协会(BSI)制订的信息安全管理体系标准 BS 7799 分为两大部分，即 BS 7799-Part 1 及 BS 7799-Part 2。这个标准为企业及各种组织进行信息安全管理提供了一个完整的管理框架。信息安全管理标准引导企业或组织建立一个完整的信息安全管理体系，对信息安全进行动态的管理，以分析企业或组织面临的安全风险为起点，对企业的信息安全风险进行动态的、全面的、有效的、不断改进的管理，并强调信息安全管理的目的是保持企业或组织业务的连续性不受信息安全事件的破坏，要从企业或组织现有的资源和管理基础为出发点，建立信息安全管理体系(ISMS)，不断改进信息安全管理的水平，使企业或组织的信息安全以最小代价达到需要的水准。

保护信息安全，建立信息安全管理体系是保障企业及组织安全营运的重要工作之一。BS 7799-Part 2 是目前建立信息安全管理体系最重要的参考依据，它以“计划(Plan)、实施(Do)、检查(Check)、行动(Action)”模式，将管理体系规范导入企业或组织，以达到“持续改进”的目的。

随着在世界范围内信息化水平的不断发展和贸易全球一体化的不断普及和深入，信息系统在企业和组织中得到了广泛的应用。许多企业对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使得信息安全管理成为企业管理越来越关键的一部分；在很多的场合，它已经成为一个企业或组织生死存亡或贸易亏盈成败中起决定性的因素，因此信息安全逐渐成为人们关注的焦点。世界范围内的各国家、机构、组织、个人都在探寻如何保障信息安全的问题，各相关部门和研究机构也纷纷投入相当的人力、物力和资金试图来解决信息安全问题。

在企业的管理者想方设法保障本企业的信息安全的同时，破坏者也道高一尺、魔高一丈，数不胜数的计算机病毒、防不胜防的电脑黑客、各类层出不穷的泄密事故就是明证。就拿中国来说，近年来也接连不断地出现了程度不同的信息安全事件，这些事件不仅仅是简单的信息系统瘫痪的问题，其直接后果是导致巨大的经济损失，还造成了不良的社会影响。如果说经济损失还能弥补，那么由于信息网络的脆弱性而引起的公众对网络社会的诚信危机则不是短时期内可能恢复的。

安全是一种“买不到”的东西。打开包装箱后即插即用，并提供足够安全水平的安全防护体系是不存在的。因此，许多企业虽然安装了一些安全产品，但并不等于拥有了一个真正的安全体系。相关调查数据显示，超过 75%的信息系统泄密和恶意攻击事件都是人为造成的，即由于信息安全管理的缺位而造成的。而技术本身实际上只是信息安全体系里的一小部分。不管一项技术有多先进，都只不过是辅助实现信息安全的手段而已。大部分的信息安全管理专家认为技术并不是不重要，但在信息安全的架构里，它一定要建立在好的信息安全管理体系的基础上，所以在业界中一向有三分技术，七分管理的说法。

正是在这样的世界大环境和学术界共同认同的原则下，各国的研究机构都纷纷研究和制订信息安全管理、风险评估、信息安全技术的标准。而英国标准化协会(BSI)，这个在全世界标准界负有盛名的机构，在成功地制订了 ISO 9000、ISO 14000、OHSAS 18000 等国际

著名的标准后，又在信息安全管理领域夺得头筹，它制订的 BS 7799 信息安全管理标准再一次成为国际上最具权威的和最具代表性的标准。

早在 1995 年 2 月，英国标准协会(BSI)就提出制订信息安全管理标准，并迅速于 1995 年 5 月制订完成，并且于 1999 年重新修改了该标准。BS 7799 分为两个部分：《信息安全管理实施规则》(BS 7799-Part 1)和《信息安全管理体系规范》(BS 7799-Part 2)。《信息安全管理实施规则》于 2000 年 12 月通过 ISO/IECJTC1(国际标准化组织和国际电工委员会的联合技术委员会)认可，正式成为国际标准，即 ISO/IEC 17799:2000《信息技术-信息安全管理实施细则》。这是通过 ISO 表决最快的一个标准，足见世界各国对该标准的关注和接受程度。2002 年 9 月 5 日，英国标准化协会又发布了新版本 BS 7799-Part 2。

7.4.2 BS 7799-Part 1 与 BS 7799-Part 2 的关系

《信息安全管理实施细则》(BS 7799-Part 1)是企业建立并实施信息安全管理体系的一个指导性的准则，主要为企业制订其信息安全策略和进行有效的信息安全控制提供了一个大众化的最佳范例。《信息安全管理体系规范》(BS 7799-Part 2)规定了建立、实施和文件化信息安全管理体系(ISMS)的要求，规定了根据独立企业的需要应实施安全控制的要求。正如该标准的适用范围介绍的一样，本标准适用以下场合：企业按照本标准要求建立并实施信息安全管理体系，进行有效的信息安全风险管理，确保商务可持续性发展；作为寻求信息安全管理体系第三方认证的标准。BS 7799-Part 2 明确提出信息安全管理要求，BS 7799-Part 1 则对应给出了通用的控制方法(措施)，因此，BS 7799-Part 2 才是认证的依据。严格地说，企业获得的认证是获得了 BS 7799-Part 2 的认证，BS 7799-Part 1 为 BS 7799-Part 2 的具体实施提供了指南，但标准中的控制目标、控制方式的要求并非信息安全管理的全部，企业可以根据需要考虑另外的控制目标和控制方式。

7.4.3 《信息安全管理实施细则》(BS 7799-Part 1)的主要内容

BS 7799-Part 1 标准在正文中“对什么是信息安全、为什么需要信息安全、如何确定安全需要、评估安全风险、选择控制措施、信息安全起点、关键的成功因素、制定自己的准则”等内容作了说明。

在 BS 7799-Part 1 标准中指出，信息安全(Information security)是指信息的保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)的保持。保密性定义为保障信息仅仅为那些被授权使用的人获取。完整性定义为保护信息及其处理方法的准确性和完整性。可用性定义为保障授权使用人在需要时可以获取信息和使用相关的资产。

标准在解释“为什么需要信息安全”时指出，信息、信息处理过程及对信息起支持作用的信息系统和信息网络都是重要的商务资产。信息的保密性、完整性和可用性对保持竞争优势、资金流动、效益、法律符合性和商业形象都是至关重要的。然而，越来越多的企业的信息系统和网络面临着包括计算机诈骗、间谍、蓄意破坏、火灾、水灾等大范围的安全威胁，诸如计算机病毒、计算机入侵、DOS 攻击等手段造成的信息灾难已变得更加普遍，有计划而不易被察觉。企业对信息系统和信息服务的依赖意味着更易受到安全威胁的破坏，公共和私人网络的互连及信息资源的共享增大了实现访问控制的难度。许多信息系统本身就不是按照

安全系统的要求来设计的，所以仅依靠技术手段来实现信息安全有其局限性，所以信息安全的实现必须得到管理和程序控制的适当支持。

该标准的正文规定了127个安全控制措施，来帮助企业识别在运作过程中对信息安全有影响的元素，企业可以根据适用的法律法规和章程加以选择和使用，或者增加其他附加控制。如图7-11所示，信息安全管理系统的127个安全控制措施被分成11个方面，构成企业实施的信息安全管理系统的结构。

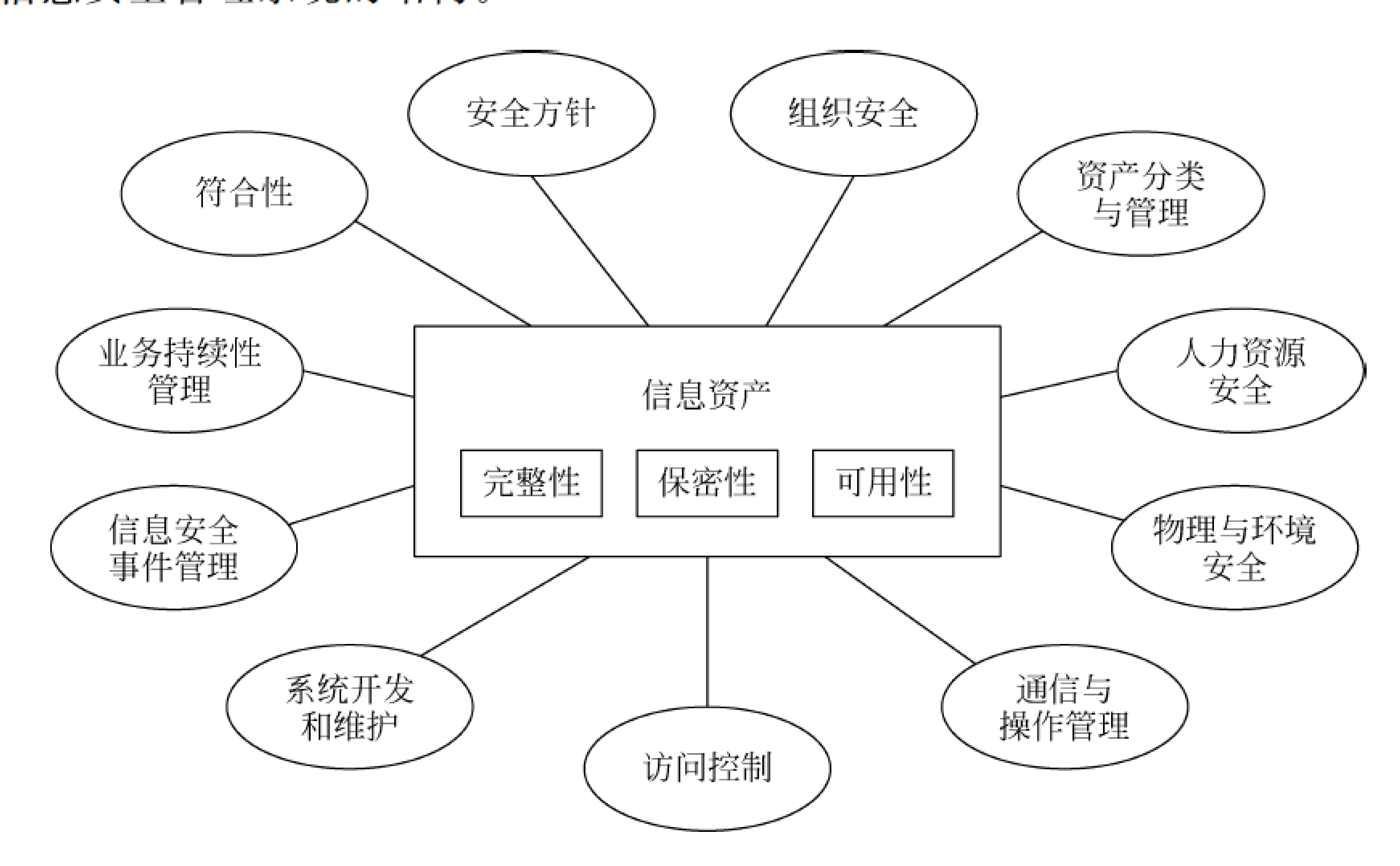


图7-11　信息安全管理系统的结构

1. 安全方针

制定信息安全方针，为信息安全提供管理指导和支持。

2. 组织安全

建立信息安全基础设施，来管理组织范围内的信息安全；维持被第三方所访问的组织的信息处理设施和信息资产的安全，以及当信息处理外包给其他组织时，维护信息的安全。

3. 资产的分类与控制

核查所有信息资产，以维护组织资产的适当保护，并做好信息分类，确保信息资产受到适当程度的保护。

4. 人力资源安全

注意工作职责定义和人力资源中的安全，以减少人为差错、盗窃、欺诈或误用设施的风险；做好用户培训，确保用户知道信息安全威胁和事务，并准备好在其正常工作过程中支持组织的安全政策；制定对安全事故和故障的响应流程，使安全事故和故障的损害减到最小，并监视事故和从事故中学习。

5. 物理和环境的安全

定义安全区域，以避免对业务办公场所和信息的未授权访问、损坏和干扰；保护设备的安全，防止信息资产的丢失、损坏或泄露和业务活动的中断；同时还要做好一般控制，以防止信息和信息处理设施的泄露或盗窃。

6. 通信和操作管理

制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统故障的风险减低到最小；防范恶意软件，保护软件和信息的完整性；建立内务规程，以维护信息处理和通信服务的完整性和可用性；确保信息在网络中的安全，以及保护其支持基础设施；建立媒体处置和安全的规程，防止资产损坏和业务活动的中断；防止信息和软件在组织之间交换时丢失、修改或误用。

7. 访问控制

制定访问控制的业务要求，以控制对信息的访问；建立全面的用户访问管理，避免信息系统的未授权访问；让用户了解他对维护有效访问控制的职责，防止未授权用户的访问；对网络访问加以控制，保护网络服务；建立操作系统级的访问控制，防止对计算机的未授权访问；建立应用访问控制，防止未授权用户访问保存在信息系统中的信息；监视系统访问和使用，检测未授权的活动；当使用移动计算和远程工作时，也要确保信息安全。

8. 信息安全事故管理

报告信息安全事件；报告信息安全弱点；确保与信息系统有关的安全事件和弱点的沟通能够及时采取纠正措施。收集证据，从信息安全事故中学习，确保使用持续有效的方法管理信息安全事故。

9. 系统开发和维护

标识系统的安全要求，确保安全被构建在信息系统内；控制应用系统的安全，防止应用系统中用户数据的丢失、被修改或误用；使用密码控制，保护信息的保密性、真实性或完整性；控制对系统文件的访问，确保按安全方式进行 IT 项目和支持活动；严格控制开发和支持过程，维护应用系统软件和信息的安全。

10. 业务持续性管理

业务持续性管理的目的是为了减少业务活动的中断，使关键业务过程免受主要故障或天灾的影响。

11. 符合性

信息系统的设计、操作、使用和管理要符合法律要求，避免任何犯罪、违反法律、违背法规、规章或合约义务以及任何安全要求；定期审查安全政策和技术符合性，确保系统符合企业安全政策和标准；还要控制系统审核，使系统审核过程的效力最大化，干扰最小化。

7.4.4 《信息安全管理体系规范》(BS 7799-Part 2)的主要内容

BS 7799-Part 2 标准详细说明了建立、实施和维护信息安全管理系统(ISMS)的要求，指出实施的企业或组织(注：以下均统称为企业)需要进行信息安全风险评估来鉴定信息系统的安全性能，并对自己的需求采取适当的控制措施。这一部分提出了企业建立信息安全管理体系的步骤，如图 7-12 所示。



图 7-12　建立信息安全管理体系的步骤

1. 定义信息安全策略

信息安全策略是企业信息安全的最高方针，需要根据企业内各个部门的实际情况，分别制订不同的信息安全策略。例如，规模较小的企业可能只有一个信息安全策略，并适用于企业内所有部门、员工；而规模较大的集团企业则需要制订一个信息安全策略文件，分别适用于不同的子公司或各分支机构。信息安全策略应该简单明了、通俗易懂，并形成书面文件，发给企业内的所有成员。同时要对所有相关员工进行信息安全策略的培训，对信息安全负有特殊责任的人员要进行特殊的培训，以使信息安全方针真正植根于企业内所有员工的脑海，并且落实到实际工作中。

2. 定义 ISMS 的范围

ISMS 的范围确定需要重点进行信息安全管理的领域，企业需要根据自己的实际情况，在整个企业范围内，或者在个别部门或领域构架 ISMS。在本阶段，应将组织划分成不同的信息安全控制领域，以易于企业对有不同需求的领域进行适当的信息安全管理。

3. 进行信息安全风险评估

信息安全风险评估的复杂程度将取决于风险的复杂程度和受保护资产的敏感程度，所采用的评估措施应该与企业对信息资产风险的保护需求相一致。风险评估主要对 ISMS 范围内的信息资产进行鉴定和估价，然后对信息资产面对的各种威胁和脆弱性进行评估，同时对已存在的或规划的安全管制措施进行鉴定。风险评估主要依赖于商业信息和系统的性质、使用信息的商业目的、所采用的系统环境等因素，企业在进行信息资产风险评估时，需要

将直接后果和潜在后果一并考虑。

4. 信息安全风险管理

根据风险评估的结果进行相应的风险管理。信息安全风险管理主要包括以下几种措施。

(1) 降低风险：在考虑转嫁风险前，应首先考虑采取措施降低风险。

(2) 避免风险：有些风险很容易避免，例如通过采用不同的技术、更改操作流程、采用简单的技术措施等。

(3) 转嫁风险：通常只有当风险不能被降低或避免且被第三方(被转嫁方)接受时才被采用。一般用于那些低概率、但一旦风险发生时会对企业产生重大影响的风险。

(4) 接受风险：用于那些在采取了降低风险和避免风险措施后，出于实际和经济方面的原因，只要企业进行运营，就必然存在必须接受的风险。

5. 确定管制目标和选择管制措施

管制目标的确定和管制措施的选择原则是费用不超过风险所造成的损失。由于信息安全是一个动态的系统工程，企业应实时对选择的管制目标和管制措施加以校验和调整，以适应变化了的情况，使企业的信息资产得到有效、经济、合理的保护。

6. 准备信息安全适用性声明

信息安全适用性声明记录了企业内相关的风险管制目标和针对每种风险所采取的各种控制措施。信息安全适用性声明的准备，一方面是为了向企业内的员工声明对信息安全面对的风险的态度，在更大程度上则是为了向外界表明企业的态度和作为，以表明企业已经全面、系统地审视了企业的信息安全系统，并将所有有必要管制的风险控制在能够被接受的范围内。

7.4.5 PDCA 过程模式

信息安全管理体系的基础是 PDCA 过程模式的应用，而 PDCA 过程模式的理论基础是戴明环，包括计划(Plan)、实施(Do)、检查(Check)和改进(Action)4 个步骤。

(1) 计划(Plan)：根据风险评估结果、法律法规要求、企业自身业务运作需要来确定控制目标与控制措施。

(2) 实施(Do)：实施所选的安全控制措施。

(3) 检查(Check)：依据策略、程序、标准和法律法规，对安全措施的实施情况进行符合性检查。

(4) 改进(Action)：根据 ISMS 审核、管理评审的结果及其他相关信息，采取纠正和预防措施，实现 ISMS 的持续改进。

这四个步骤组成一个闭合的戴明环，通过这个环的不断运转，使信息安全管理体系得到持续改进，使信息安全绩效(performance)螺旋上升。戴明环的结构如图 7-13 所示。

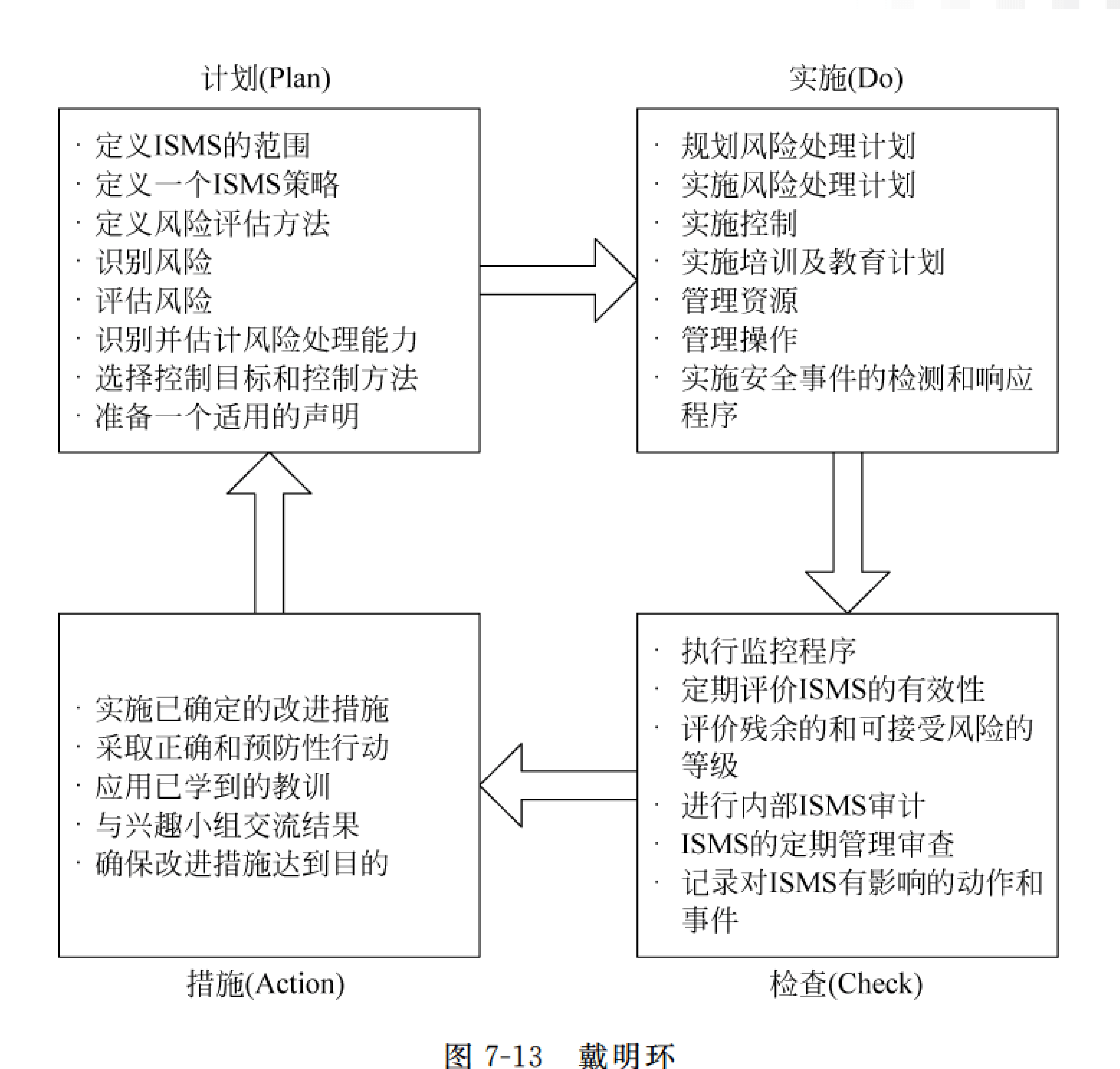


图 7-13　戴明环

1. 计划 P——建立信息安全管理体系环境和风险评估体系

要启动 PDCA 循环，必须有“启动器”，如提供必需的资源、选择风险管理方法、确定评审方法、文件化实践。设计计划阶段就是为了确保正确建立信息安全管理体系的范围和详略程度，识别并评估所有的信息安全风险，为这些风险制订适当的处理计划。计划阶段的所有重要活动都要被文件化，以备将来追溯和控制更改情况。

1）确定范围和方针

信息安全管理体系可以覆盖企业的全部或者部分。无论是全部还是部分，企业都必须明确界定体系的范围，如果体系仅涵盖企业的一部分这就变得更重要了。企业需要文件化信息安全管理体系的范围，信息安全管理体系范围文件应该涵盖包括确立信息安全管理体系范围和体系环境所需的过程；战略性和组织化的信息安全管理环境；企业的信息安全风险管理方法；信息安全风险评价标准以及所要求的保证程度；信息资产识别的范围等几个方面。

信息安全管理体系也可能在其他信息安全管理体系的控制范围内。在这种情况下，上下级控制的关系有下列两种可能：

（1）下级信息安全管理体系不使用上级信息安全管理体系的控制。在这种情况下，上级信息安全管理体系的控制不影响下级信息安全管理体系的 PDCA 活动。

（2）下级信息安全管理体系使用上级信息安全管理体系的控制。在这种情况下，上级信息安全管理体系的控制可以被认为是下级信息安全管理体系策划活动的“外部控制”。尽管此类外部控制并不影响下级信息安全管理体系的实施、检查、措施活动，但是下级信息安

全管理体系仍然有责任确认这些外部控制提供了充分的保护。

安全方针是关于在一个组织内，指导如何对信息资产进行管理、保护和分配的规则和指示，是企业信息安全管理体系的基本法规。企业的信息安全方针，描述信息安全在企业内的重要性，表明管理层的承诺，提出企业管理信息安全的方法，为企业的信息安全管理提供方向和支持。

2）定义风险评估的系统性方法

确定信息安全风险评估方法，并确定风险等级准则。评估方法应该和企业既定的信息安全管理体系范围、信息安全需求、法律法规要求相适应，兼顾效果和效率。企业需要建立风险评估文件，解释所选择的风险评估方法、说明为什么该方法适合企业的安全要求和业务环境，介绍所采用的技术和工具，以及使用这些技术和工具的原因。评估文件还应该规范下列评估细节：

（1）信息安全管理体系内资产的估价，包括所用的价值尺度信息；

（2）威胁及薄弱点的识别；

（3）可能利用薄弱点的威胁的评估，以及此类事故可能造成的影响；

（4）以风险评估结果为基础的风险计算，以及剩余风险的识别。

3）识别风险

识别信息安全管理体系控制范围内的信息资产；识别对这些资产的威胁；识别可能被威胁利用的薄弱点；识别保密性、完整性和可用性丢失对这些资产的潜在影响。

4）评估风险

根据资产保密性、完整性或可用性丢失的潜在影响，评估由于安全失败（failure）可能引起的商业影响；根据与资产相关的主要威胁、薄弱点及其影响，以及目前实施的控制，评估此类失败发生的现实可能性；根据既定的风险等级准则，确定风险等级。

5）识别并评价风险处理的方法

对于所识别的信息安全风险，企业需要加以分析，区别对待。如果风险满足企业的风险接受方针和准则，那么就有意的、客观的接受风险；对于不可接受的风险企业可以考虑避免风险或者将风险转移；对于不可避免也不可转移的风险应该采取适当的安全控制措施，将其降低到可接受的水平。

6）为风险的处理选择控制目标与控制方式

选择并文件化控制目标和控制方式，以将风险降低到可接受的等级。BS 7799-2：2002 附录 A 提供了可供选择的控制目标与控制方式。不可能总是以可接受的费用将风险降低到可接受的等级，那么需要确定是增加额外的控制，还是接受高风险。在设定可接受的风险等级时，控制的强度和费用应该与事故的潜在费用相比较。这个阶段还应该策划安全破坏或者违背的探测机制，进而安排预防、制止、限制和恢复控制。在形式上，企业可以通过设计风险处理计划来完成步骤 5）和 6）。风险处理计划是企业针对所识别的每一项不可接受风险建立的详细处理方案和实施时间表，是企业安全风险和控制措施的接口性文档。风险处理计划不仅可以指导后续的信息安全管理活动，还可以作为与高层管理者、上级领导机构、合作伙伴或者员工进行信息安全事宜沟通的桥梁。这个计划至少应该为每一个信息安全风险阐明以下内容：企业所选择的处理方法；已经到位的控制；建议采取的额外措施；建议控制的实施时间框架。

7）获得最高管理者的授权批准

剩余风险(residual risks)的建议应该获得批准，开始实施和运作信息安全管理体系需要获得最高管理者的授权。

2. 实施 D——实施并运行

PDCA 循环中这个阶段的任务是以适当的优先权进行管理运作，执行所选择的控制，以管理策划阶段所识别的信息安全风险。对于那些被评估认为是可接受的风险，不需要采取进一步的措施。对于不可接受风险，需要实施所选择的控制，这应该与策划活动中准备的风险处理计划同步进行。计划的成功实施需要有一个有效的管理系统，其中要规定所选择方法、分配职责和职责分离，并且要依据规定的方式方法监控这些活动。

在不可接受的风险被降低或转移之后，还会有一部分剩余风险。应对这部分风险进行控制，确保不期望的影响和破坏被快速识别并得到适当管理。本阶段还需要分配适当的资源（人员、时间和资金）运行信息安全管理体系以及所有的安全控制。这包括将所有已实施控制的文件化，以及信息安全管理体系文件的积极维护。

提高信息安全意识的目的就是产生适当的风险和安全文化，保证意识和控制活动的同步，还必须安排针对信息安全意识的培训，并检查意识培训的效果，以确保其持续有效和实时性。如有必要应对相关方事实有针对性的安全培训，以支持组织的意识程序，保证所有相关方能按照要求完成安全任务。本阶段还应该实施并保持策划了的探测和响应机制。

3. 检查 C——监视并评审

1）检查阶段

检查阶段又叫学习阶段，是 PDCA 循环的关键阶段，是信息安全管理体系要分析运行效果，寻求改进机会的阶段。如果发现一个控制措施不合理、不充分，就要采取纠正措施，以防止信息系统处于不可接受风险状态。企业应该通过多种方式检查信息安全管理体系是否运行良好，并对其业绩进行监视，可能包括下列管理过程：

(1) 执行程序和其他控制以快速检测处理结果中的错误；快速识别安全体系中失败的和成功的破坏活动；能使管理者确认人工或自动执行的安全活动达到预期的结果；按照商业优先权确定解决安全破坏所要采取的措施；接受其他企业和企业自身的安全经验。

(2) 常规评审信息安全管理体系的有效性；收集安全审核的结果、事故以及来自所有股东和其他相关方的建议和反馈，定期对信息安全管理体系有效性进行评审。

(3) 评审剩余风险和可接受风险的等级；注意企业、技术、商业目标和过程的内部变化，以及已识别的威胁和社会风尚的外部变化，定期评审剩余风险和可接受风险等级的合理性。

(4) 审核是执行管理程序、以确定规定的安全程序是否适当、是否符合标准以及是否按照预期的目的进行工作。审核的就是按照规定的周期（最多不超过一年）检查信息安全管理体系的所有方面是否行之有效。审核的依据包括 BS 7799-2:2002 标准和企业所发布的信息安全管理程序。应该进行充分的审核策划，以便审核任务能在审核期间内按部就班的展开。

2）评审阶段

评审阶段的主要审核以下几项内容：

(1) 信息安全方针仍然是业务要求的正确反映。

(2) 正在遵循文件化的程序(信息安全管理体系范围内)，并且能够满足其期望的目标。

(3) 有适当的技术控制(例如防火墙、实物访问控制)，被正确的配置，且行之有效。

(4) 剩余风险已被正确评估，并且是企业管理可以接受的。

(5) 前期审核和评审所认同的措施已经被实施。

(6) 审核会包括对文件和记录的抽样检查，以及口头审核管理者和员工。

(7) 正式评审：为确保范围保持充分性，以及信息安全管理体系过程的持续改进得到识别和实施，企业应定期对信息安全管理体系进行正式的评审(最少一年评审一次)。记录并报告能影响信息安全管理体系有效性或业绩的所有活动和事件。

4. 改进 A——措施及改进

经过了策划、实施、检查之后，企业在改进阶段必须对所策划的方案给以结论，是应该继续执行，还是应该放弃重新进行新的策划。当然该循环给管理体系带来明显的业绩提升，企业可以考虑是否将成果扩大到其他的部门或领域，这就开始了新一轮的 PDCA 循环。在这个过程中企业可能持续进行以下操作：

(1) 测量信息安全管理体系满足安全方针和目标方面的业绩。

(2) 识别信息安全管理体系的改进，并有效实施。

(3) 采取适当的纠正和预防措施。

(4) 沟通结果及活动，并与所有相关方磋商。

(5) 必要时修订信息安全管理体系。

(6) 确保修订达到预期的目标。

在这个阶段需要注意的是，很多看起来单纯的、孤立的事件，如果不及时处理就可能对整个企业产生影响，所采取的措施不仅具有直接的效果，还可能带来深远的影响。企业需要把措施放在信息安全管理体系持续改进的大背景下，以长远的眼光来打算，确保措施不仅致力于眼前的问题，还要杜绝类似事故再发生或者降低其在放生的可能性。

不符合、纠正措施和预防措施是本阶段的重要概念。

不符合是指实施、维持并改进所要求的一个或多个管理体系要素缺乏或者失效，或者是在客观证据基础上，信息安全管理体系符合安全方针以及达到企业安全目标的能力存在很大不确定性的情况。

纠正措施是企业应确定措施，以消除信息安全管理体系实施、运作和使用过程中不符合的原因，防止再发生。组织的纠正措施的文件化程序应该规定以下方面的要求：

① 识别信息安全管理体系实施、运作过程中的不符合。

② 确定不符合的原因。

③ 评价确保不符合不再发生的措施要求。

④ 取定并实施所需的纠正措施。

⑤ 记录所采取措施的结果。

⑥ 评审所采取措施的有效性。

预防措施是企业应确定措施,以消除潜在不符合的原因,防止其发生。预防措施应与潜在问题的影响程度相适应。预防措施的文件化程序应该规定以下方面的要求:

① 识别潜在不符合及其原因。

② 确定并实施所需的预防措施。

③ 记录所采取措施的结果。

④ 评审所采取的预防措施。

⑤ 识别已变化的风险,并确保对发生重大变化的风险予以关注。

7.4.6 中国信息安全管理标准

中国政府主管部门以及各行各业已经认识到了信息安全的重要性。政府部门出台了一系列的相关政策,直接牵引、推进信息安全的应用和发展。由政府主导的各大信息系统工程和信息化程度要求非常高的相关行业,也开始出台对信息安全技术产品的应用标准和规范。国务院信息化工作小组颁布的《关于我国电子政务建设指导意见》也强调指出了电子政务建设中信息系统安全的重要性;中国人民银行正在加紧制订网上银行系统安全性评估指引,并明确提出对信息安全的投资要达到 IT 总投资的 10%以上,而在其他一些关键行业,信息安全的投资甚至已经超过了总 IT 预算的 30%~50%。

2002 年 4 月,中国成立了“全国信息安全标准化技术委员会(TC260)”,该标委会是在信息安全的专业领域内,从事信息安全标准化工作的技术工作组织。信息安全标委会设置了 10 个工作组,其中信息安全管理(含工程与开发)工作组(WG7)负责对信息安全的行政、技术、人员等管理提出规范要求及指导指南,它包括信息安全管理指南、信息安全管理实施规范、人员培训教育及录用要求、信息安全社会化服务管理规范、信息安全保险业务规范框架和安全策略要求与指南。目前,WG7 工作组正在着手制订推荐性国家标准《信息技术信息安全管理实用规则》,该标准的采用程度为等同采用标准,也就是说该标准与 ISO/IEC 17799 相同,除了纠正排版或印刷错误、改变标点符号、增加不改变技术内容的说明和指示之外不改变标准技术的内容。

BS 7799 提供了一套综合的、由信息安全最佳措施组成的实施规则和管理要求,它广泛地涵盖了几乎所有的安全议题,非常适合于作为工商业及大、中、小组织的信息系统在大多数情况下所需的控制范围确定的参考基准。虽然我国信息安全标准委员会并不是将 ISO/IEC 17799 作为强制性国家标准引入,而是仅仅作为推荐性国家标准推行,但是企业和组织仍然可以将 ISO/IEC 17799 作为衡量信息安全管理体系规范程度的一个标准和指标。建立信息安全管理体系并获得经认可的认证机构的认证,不仅能提高企业自身的安全管理水平,将企业的安全风险控制在可接受的程度,减小信息安全遭到破坏带来的损失,保证业务的可持续运作;并且能向客户及利益相关方展示组织对信息安全的承诺,增强投资方和股票持有者的投资信息,向政府及行业主管部门证明组织对相关法律法规的符合,并且得到国际上的承认。尤其对于银行、证券、电子商务、ISP 等服务提供商来说,可以借此向客户展示其服务相比其他竞争对手更加安全、可靠,并树立和增强企业的信息安全角度,提高企业的综合竞争力。

7.5 物联网安全风险评估

在信息安全领域，对信息系统进行风险评估十分重要，其最终目的就是要指导决策者在“投资成本”和“安全级别”这两者之间找到平衡，从而为等级化的资产风险制订保护策略和缓和计划。信息安全风险评估方法经历了从手工评估到半自动化评估的阶段，目前正在由技术评估向整体评估发展，由定性评估向定性和定量评估相结合的方法发展，由基于知识的评估向基于模型的评估方法发展。

7.5.1 风险的概念

风险是指信息系统遭受损害或者损失的可能性，是实现一个事件不想要的负面结果的潜在因素。早在 1992 年，Ansell，J. 和 F. Wharton 提出了以下的风险数学表达式：

$$风险\ R = f(p,c)$$

其中：p 为事件发生的概率，c 为事件发生的后果。

风险分析是风险评估过程中最复杂的步骤，要求对风险的识别、估计和评价做出全面的、综合的分析。一个全面的风险分析包括对各种层次的风险发生的概率和影响进行评价。风险评估重点关注风险的评估和量化，由此决定风险的可接受级别。

风险管理过程定义了综合的策略来解决风险分析过程中识别出来的风险。Britton 等人提出了三种基本的风险解决办法：接受风险、减小风险和转移风险。

在信息安全系统中，威胁、脆弱点、资产和影响之间的关系如图 7-14 所示。

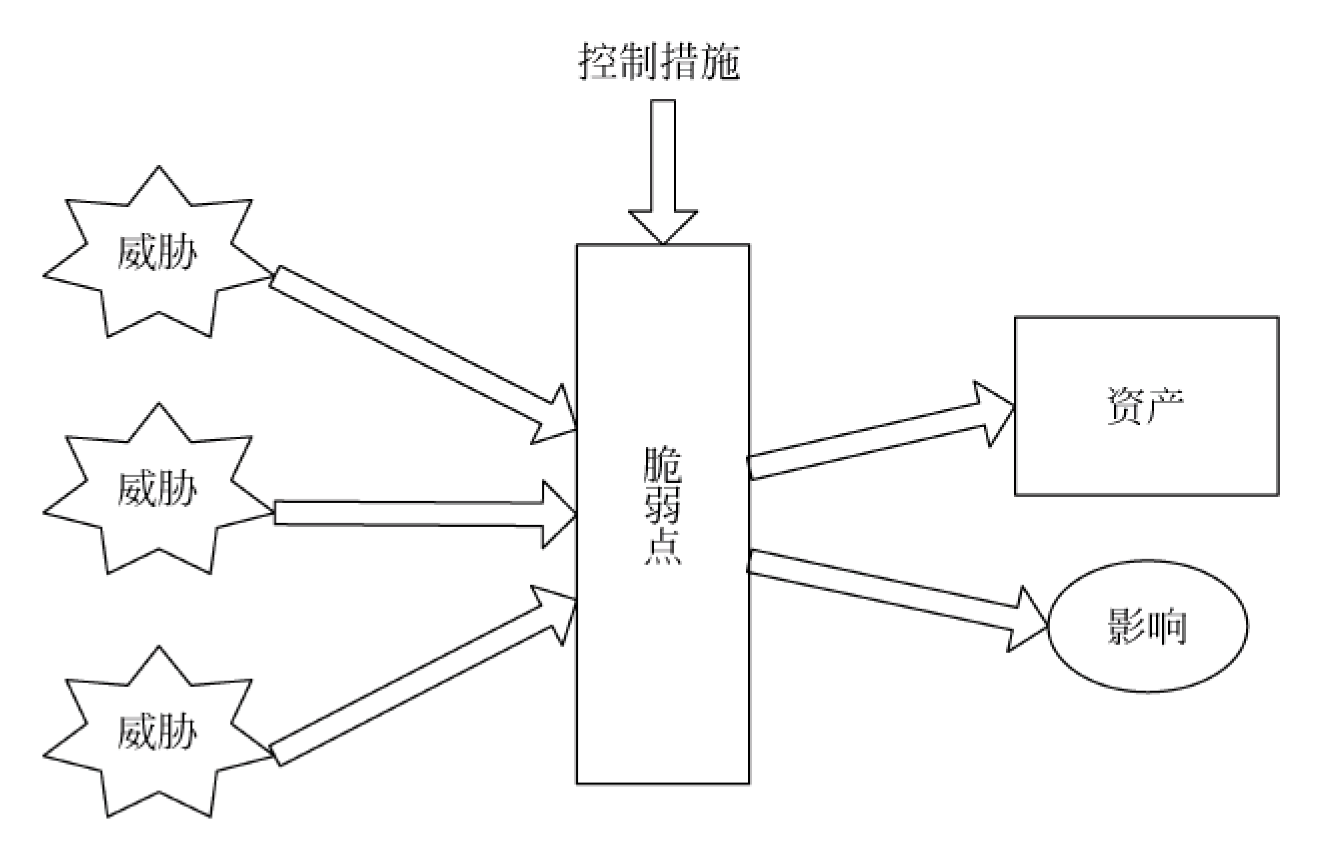


图 7-14 威胁、脆弱点、资产和影响之间的关系

7.5.2 常用信息安全风险评估方法

面对信息安全问题时，需要从企业的角度去评估他们实际上需要保护什么及其需求的原因。大多数安全问题深深地根植在一个或者多个企业和业务问题中。在实施安全方案之前，应当通过在业务环境中评估安全需求和风险，刻画出基本问题的真实本质，决定需要保护哪些对象，为什么要保护这些对象，需要从哪些方面进行保护，如何在生存期内进行保护。

下面将从不同的角度比较现有的信息安全风险评估方法。

1. 手工评估与工具辅助评估

在各种信息安全风险评估工具出现以前，对信息系统进行安全管理，一切工作都只能手工进行。对于安全风险分析人员而言，这些工作包括识别重要资产、安全需求分析、当前安全实践分析、威胁和弱点发现、基于资产的风险分析和评估等。对于安全决策者而言，这些工作包括资产估价、安全投资成本以及风险效益之间的平衡决策等。对于系统管理员而言，这些工作包括基于风险评估的风险管理等。总而言之，其劳动量巨大，容易出现疏漏，而且，他们都是依据各自的经验，进行与安全风险相关的工作。

风险评估工具的出现在一定程度上解决了手动评估的局限性。

1985 年，英国 CCTA 公司开发了 CRAMM 风险评估工具。CRAMM 包括全面的风险评估工具，并且完全遵循 BS 7799 规范，包括依靠资产的建模、商业影响评估、识别和评估威胁和弱点、评估风险等级、识别需求和基于风险评估调整控制等。CRAMM 评估风险依靠资产价值、威胁和脆弱点，这些参数值是通过 CRAMM 评估者与资产所有者、系统使用者、技术支持人员和安全部门人员一起的交互活动得到，最后给出一套安全解决方案。

1991 年，C&A System Security 公司推出了 COBRA 工具，用来进行信息安全风险评估。COBRA 由一系列风险分析、咨询和安全评价工具组成，它改变了传统的风险管理方法，提供了一个完整的风险分析服务，并且兼容许多风险评估方法学(如定性分析和定量分析等)。它可以看作一个基于专家系统和扩展知识库的问卷系统，对所有的威胁和脆弱点评估其相对重要性，并且给出合适的建议和解决方案。此外，它还对每个风险类别提供风险分析报告和风险值(或风险等级)。

信息安全风险评估工具的出现，大大缩短了风险评估所花费的时间。在系统应用和配置不断改变的情况，企业可以通过执行另外一次评估重新设置风险基线。两次评估的时间间隔可以预先确定(例如，以月为单位)或者由主要的事件触发(例如，企业重组、企业的计算基础结构重新设计等)。

2. 技术评估和整体评估

技术评估是指对企业的技术基础结构和程序进行系统的、及时的检查，包括对企业内部计算环境的安全性及其对内外攻击脆弱性的完整性攻击。这些技术驱动的评估通常包括：

(1) 评估整个计算基础结构。

(2) 使用拥有的软件工具分析基础结构及其全部组件。

(3) 提供详细的分析报告，说明检测到的技术弱点，并且可能为解决这些弱点建议具体的措施。技术评估是通常意义上所讲的技术脆弱性评估，强调企业的技术脆弱性。但是企业的安全性遵循“木桶原则”，仅仅与企业内最薄弱的环节相当，而这一环节多半是企业中的某个人。

整体风险评估扩展了上述技术评估的范围，着眼于分析企业内部与安全相关的风险，包括内部和外部的风险源、技术基础和组织结构以及基于电子的和基于人的风险。这些多角度的评估试图按照业务驱动程序或者目标对安全风险进行排列，关注的焦点主要集中在安全的 4 个方面。

(1) 检查与安全相关的企业实践，标识当前安全实践的优点和弱点。这一程序可能包括对信息进行比较分析，根据工业标准和最佳实践对信息进行等级评定。

(2) 包括对系统进行技术分析、对政策进行评审以及对物理安全进行审查。

(3) 检查 IT 的基础结构，以确定技术上的弱点。包括恶意代码的入侵、数据的破坏或者毁灭、信息丢失、拒绝服务、访问权限和特权的未授权变更等。

(4) 帮助决策制订者综合平衡风险以选择成本效益对策。

1999 年，卡内基·梅隆大学的 SEI 发布了 OCTAVE 框架，这是一种自主型信息安全风险评估方法。OCTAVE 方法是 Alberts 和 Dorofee 共同研究的成果，这是一种从系统的、企业的角度开发的新型信息安全保护方法，主要针对大型企业，中小型企业也可以对其适当裁剪，以满足自身需要。它的实施分为三个阶段：

(1) 建立基于资产的威胁配置文件(Threat Profile)。这是从企业的角度进行的评估。企业的全体员工阐述他们的看法，如什么对企业重要(与信息相关的资产)，应当采取什么样的措施保护这些资产等。分析团队整理这些信息，确定对企业最重要的资产(关键资产)并标识对这些资产的威胁。

(2) 标识基础结构的弱点。对计算基础结构进行的评估。分析团队标识出与每种关键资产相关的关键信息技术系统和组件，然后对这些关键组件进行分析，找出导致对关键资产产生未授权行为的弱点(技术弱点)。

(3) 开发安全策略和计划。分析团队标识出企业关键资产的风险，并确定要采取的措施。根据对收集到的信息所做的分析，为企业开发保护策略和缓和计划，以解决关键资产的风险。

3. 定性评估和定量评估

定性分析方法是最广泛使用的风险分析方法。该方法通常只关注威胁事件所带来的损失(Loss)，而忽略事件发生的概率(Probability)。多数定性风险分析方法依据企业面临的威胁、脆弱点以及控制措施等元素来决定安全风险等级。在定性评估时并不使用具体的数据，而是指定期望值，如设定每种风险的影响值和概率值为“高”、“中”、“低”。有时单纯使用期望值，并不能明显区别风险值之间的差别。可以考虑为定性数据指定数值。例如，设“高”的值为 3，“中”的值为 2，“低”的值为 1。但是要注意的是，这里考虑的只是风险的相对等级，并不能说明该风险到底有多大。所以，不要赋予相对等级太多的意义，否则，将会导致错误的决策。

定量分析方法利用两个基本的元素：威胁事件发生的概率和可能造成的损失。把这两个元素简单相乘的结果称为 ALE(Annual Loss Expectancy)或 EAC(Estimated Annual Cost)。理论上可以依据 ALE 计算威胁事件的风险等级，并且做出相应的决策。James W. Meritt 提出了一种定量风险评估方法。该方法首先评估特定资产的价值 V，把信息系统分解成各个组件，这样更加有利于整个系统的定价，一般按功能单元进行分解；其次根据客观数据计算威胁的频率 P；最后计算威胁影响系数 μ，因为对于每一个风险，并不是所有的资产所遭受的危害程度都是一样的，程度的范围可能从无危害到彻底危害(即完全破坏)。根据上述三个参数，并通过以下公式计算 ALE：

$$\text{ALE} = V \times P \times \mu$$

定量风险分析方法要求特别关注资产的价值和威胁的量化数据，但是这种方法存在一个问题，就是数据的不可靠和不精确。对于某些类型的安全威胁，存在可用的信息。例如，可以根据频率数据估计人们所处区域的自然灾害发生的可能性(如洪水和地震)。也可以用事件发生的频率估计一些系统问题的概率，例如系统崩溃和感染病毒。但是，对于一些其他类型的威胁来说，不存在频率数据，影响和概率很难是精确的。此外，控制和对策措施可以减小威胁事件发生的可能性，而这些威胁事件之间又是相互关联的。这将使定量评估过程非常耗时和困难。

鉴于以上难点，可以用客观概率和主观概率相结合的方法。应用于没有直接根据的情形，可能只能考虑一些间接信息、有根据的猜测、直觉或者其他主观因素，称为主观概率。应用主观概率估计由人为攻击产生的威胁需要考虑一些附加的威胁属性，如动机、手段和机会等。

4. 基于知识的评估和基于模型的评估

基于知识的风险评估方法主要是依靠经验进行的，经验从安全专家处获取并凭此来解决相似场景的风险评估问题。这种方法的优越性在于能够直接提供推荐的保护措施、结构框架和实施计划。

Parker，Donn 提出了一种基于“良好实践”的知识评估方法。该方法提出重用具有相似性企业(主要从企业的大小、范围以及市场来判断企业是否相似)的“良好实践”。为了能够较好地处理威胁和脆弱性分析，该方法开发了一个滥用和误用报告数据库，存储了 30 年来的上千个事例。同时也开发了一个扩展的信息安全框架，以辅助用户制定全面的、正确的企业安全策略。

基于知识的风险评估方法充分利用多年来开发的保护措施和安全实践，依照企业的相似性程度进行快速的安全实施和包装，以减少企业的安全风险。然而，企业相似性的判定、被评估企业的安全需求分析以及关键资产的确定都是该方法的制约点。安全风险评估是一个非常复杂的任务，这要求存在一个方法既能描述系统的细节又能描述系统的整体。

基于模型的评估可以分析出系统自身内部机制中存在的危险性因素，同时又可以发现系统与外界环境交互中的不正常并有害的行为，从而完成系统脆弱点和安全威胁的定性分析。如 UML 建模语言可以用来详细说明信息系统的各个方面：不同组件之间关系的静态图用 class diagrams 来表示；用来详细说明系统的行动和功能的动态图用 use case diagrams 和 sequence diagrams 来表示；完整的系统使用 UML diagrams 来说明，它是系统体系结构的描述。

2001 年，BITD 开始了 CORAS 工程——安全危急系统的风险分析平台。该工程旨在开发一个基于面向对象建模技术的风险评估框架，特别指出使用 UML 建模技术。利用建模技术在此主要有三个目的：第一，在合适的抽象层次描述评估目标；第二，在风险评估的不同群组中作为通信和交互的媒介；第三：记录风险评估结果和这些结果依赖的假设。CC 准则和 CORAS 方法都使用了半形式化和形式化规范。CC 准则是通用的，并不为风险评估提供方法学。然后，相对于 CC 准则而言，CORAS 为风险评估提供方法学，开发了具体的技术规范来进行安全风险评估。

总之，信息系统安全风险评估经历了从手动评估到工具辅助评估的阶段，目前正在由技

术评估到整体评估发展，由定性评估向定性和定量相结合的方向发展，由基于知识（经验）的评估向基于模型的评估方法发展。在信息系统安全应用领域，经常要求对一个企业进行信息安全风险评估。要使评估结果完整准确，必须考虑到企业的安全风险不仅仅是由计算机网络攻击所引起的，而是由技术基础结构、组织结构以及人员等综合因素所决定。也正是由于这个原因，要求信息安全风险评估必须考虑企业的方方面面的因素，同时也决定了整个评估过程非常复杂和耗时。

7.6 本章小结

物联网安全管理是指导和控制企业的关于信息安全风险的相互协调活动。关于信息安全风险的指导和控制活动，通常包括制订信息安全方针、风险评估、控制目标与方式选择、风险控制、安全保证等。而要对企业的信息安全进行高效、动态的管理，就必须依据信息安全管理模型和信息安全管理标准构建企业的信息安全管理体系。

与信息安全标准化相关的国际信息安全标准化组织包括：国际标准化组织、国际电工委员会、国际电信联盟、Internet 工程任务组。

中国的信息安全标准化组织包括：中国信息安全标准化技术委员会、公安部信息系统安全标准化技术委员会、中国通信标准化协会网络与信息安全技术工作委员会、中国传感器网络标准工作组、中国泛在网技术工作委员会、中国物联网标准联合工作组。

信息安全管理模型是对信息安全管理的一个抽象化描述。它是企业建立安全管理体系的基础。目前，在对安全理论、安全技术和安全标准研究的基础上，不同的组织都提出了相应的信息安全管理模型。这些模型的侧重点各有不同，信息安全的管理方式也不同。典型的信息安全管理模型包括 OSI 安全体系结构模型、P2DR 模型、PDRR 模型、PDCA 持续改进模型和 HTP 模型等。

2000 年 12 月，国际标准化组织 ISO 正式发布了有关信息安全的国际标准《国际信息安全管理标准体系》（ISO 17799），这个标准包括信息系统安全管理和安全认证两大部分，是参照英国国家标准 BS 7799 发展而来的。

《信息安全管理实施细则》（BS 7799-Part 1）是企业建立并实施信息安全管理体系的一个指导性的准则，主要为企业制订其信息安全策略和进行有效的信息安全控制提供了一个大众化的最佳范例。《信息安全管理体系规范》（BS 7799-Part 2）规定了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立企业的需要应实施安全控制的要求。

信息安全管理体系的基础是 PDCA 过程模式的应用，而 PDCA 过程模式的理论基础是戴明环，包括计划（Plan）、实施（Do）、检查（Check）和改进（Action）4 个步骤。

2002 年 4 月，中国成立了“全国信息安全标准化技术委员会（TC260）”，该标委会是在信息安全的专业领域内，从事信息安全标准化工作的技术工作组织。信息安全标委会设置了 10 个工作组，其中信息安全管理（含工程与开发）工作组（WG7）负责对信息安全的行政、技术、人员等管理提出规范要求及指导指南，它包括信息安全管理指南、信息安全管理实施规范、人员培训教育及录用要求、信息安全社会化服务管理规范、信息安全保险业务规范框架和安全策略要求与指南。

在信息安全领域，对信息系统进行风险评估十分重要，其最终目的就是要指导决策者在

“投资成本”和“安全级别”这两者之间找到平衡，从而为等级化的资产风险制定保护策略和缓和计划。信息安全风险评估方法经历了从手工评估到半自动化评估的阶段，目前正在由技术评估向整体评估发展，由定性评估向定性和定量评估相结合的方法发展，由基于知识的评估向基于模型的评估方法发展。

复习思考题

1. 物联网安全管理的含义是什么？
2. 信息安全管理体系的主要内容是什么？
3. 信息安全标准化组织主要包括哪些国际组织和中国组织？
4. 请简要说明各种典型的信息安全管理模型。
5. 英国 BS 7799-Part 1 标准的主要内容是什么？
6. 英国 BS 7799-Part 2 标准的主要内容是什么？
7. PDCA 过程模式的主要内容是什么？
8. 中国政府在信息安全标准化领域做了哪些工作？
9. 信息安全风险评估有哪些常用的方法？

模拟试题一

一、单项选择题(每小题 2 分,本大题共 20 分)

1. 物联网的概念最早是在(　　)年由美国麻省理工学院凯文奥斯通教授提出的。
   A. 1988　　B. 1989　　C. 1990　　D. 1991
2. 在物联网体系结构中,传感器位于物联网的(　　)层。
   A. 感知　　B. 传输　　C. 网络　　D. 应用
3. RFID 是一种(　　)识别技术。
   A. 红外线　　B. 紫外线　　C. 射频　　D. 超声波
4. ZigBee 是一种(　　)无线通信技术。
   A. 近距离　　B. 中距离　　C. 远距离　　D. 超远距离
5. IPv6 中地址长度为(　　)位。
   A. 32　　B. 64　　C. 128　　D. 256
6. 以下属于非对称加密技术的是(　　)。
   A. DES　　B. AES　　C. IDEA　　D. RSA
7. 入侵检测技术可以分为异常检测和(　　)检测两大类。
   A. 正常　　B. 误用　　C. 适用　　D. 认证
8. 无线城域网的国际标准是(　　)。
   A. 802.3　　B. 802.14　　C. 802.15　　D. 802.16
9. 云计算安全关键技术包括(　　)安全技术、海量用户的身份认证、隐私保护与数据安全技术。
   A. 云计算平台　　B. 数据管理　　C. 数据存储　　D. 虚拟机
10. BS 7799 是由(　　)提出的信息安全管理标准。
   A. 英国　　B. 德国　　C. 美国　　D. 日本

二、填空题(每小题 4 分,本大题共 20 分)

1. 物联网的四个特征是________、________、________、________。
2. 一套完整的 RFID 系统包括________、________、________、________等组成部分。
3. RFID 系统的物理安全机制包括________、________、________、________、________等五类。
4. 无线传感器网络系统通常包括________、________、________。
5. 云计算的服务可以分为三个层次:________、________、________。

三、名词解释(每小题 4 分,本大题共 20 分)

1. 对称加密算法

2. 数字签名

3. 防火墙技术

4. 数据库保护

5. 隐私

四、简答题(每小题 8 分,本大题共 40 分)

1. 请画图表示物联网的体系结构,并分别说明每一层实现的功能。

2. 请简要说明物联网云计算平台的安全机制。

3. PKI 的优势主要表现在哪些方面?

4. RFID 系统安全的密码机制包括哪些典型的安全认证协议?

5. 什么是黑客?黑客常用的攻击方法包括哪些?

模拟试题二

一、单项选择题(每小题 2 分,本大题共 20 分)

1. “感知中国”的概念是温家宝总理在(　　)年提出的。
   A. 2008　　B. 2009　　C. 2010　　D. 2011
2. 在物联网体系结构中,云计算平台位于物联网的(　　)层。
   A. 感知　　B. 传输　　C. 网络　　D. 应用
3. WiMAX 是一种无线(　　)网技术。
   A. 个域　　B. 局域　　C. 城域　　D. 广域
4. 蓝牙是一种(　　)无线通信技术。
   A. 近距离　　B. 中距离　　C. 远距离　　D. 超远距离
5. IPv4 中地址长度为(　　)位。
   A. 32　　B. 64　　C. 128　　D. 256
6. 以下属于对称加密技术的是(　　)。
   A. DES　　B. RSA　　C. 椭圆曲线　　D. ECC
7. 入侵检测技术可以分为(　　)检测和误用检测两大类。
   A. 正常　　B. 异常　　C. 适用　　D. 认证
8. 无线传感器网络网络层安全协议 SPINS 包括 SNEP 协议和(　　)协议两部分。
   A. TESLA　　B. μTESLA　　C. LEACH　　D. Rumor
9. 从工作原理来分类,防火墙可以分为四类:网络级防火墙、应用级网关、(　　)、规则检查防火墙。
   A. 感知级防火墙　　B. 感知级网关　　C. 电路级网关　　D. 软件级网关
10. 国际标准化组织(ISO)的总部位于(　　)。
   A. 伦敦　　B. 东京　　C. 纽约　　D. 日内瓦

二、填空题(每小题 4 分,本大题共 20 分)

1. 物联网系统面临的安全威胁主要包括________、________、________、________、________、________、________等七个方面。
2. 无线传感器网络分布式的密钥管理方案包括________、________和________。
3. RFID 系统的密码安全机制包括________、________、________、________、________、________等。
4. 近距离无线网络可以分为________、________、________、________、________等。
5. GPS 全球卫星定位系统包括:________、________、________等三大部分。

三、名词解释(每小题 4 分,本大题共 20 分)

1. 非对称加密算法

2. 公钥基础设施

3. 入侵检测技术

4. RFID

5. 云计算

四、简答题(每小题 8 分,本大题共 40 分)

1．请画图表示 RFID 的系统结构,并分别说明每一个组成部分的功能。

2．请简要说明 DES 算法的工作原理。

3．请简要说明哈希链(hash-chain)协议的工作原理。

4．请简要说明 RFID 中间件的工作原理。

5．什么是数据安全？数据安全的要素体现在哪些方面？

参考文献

[1] 马建峰,朱建明. 无线局域网安全——方法与技术[M]. 北京：机械工业出版社,2005.

[2] 孙利民等. 无线传感器网络. 北京：清华大学出版社,2005.5.

[3] 郎为民等. 无线传感器网络安全研究[J]. 计算机研究与发展,2005,Vol32(5):54-58.

[4] 崔莉等. 无线传感器网络研究进展[J]. 计算机研究与发展,2005,Vol142(1):163-174.

[5] 邓秀华. 计算机网络病毒的危害与防治. 电脑知识与技术,2005,27:10-12.

[6] 束红等. 信息安全相关标准的分析与研究. 网络安全技术与应用,2005,3:60-62.

[7] 吴志刚. 信息安全标准体系初探. 信息网络安全,2005,3:37.

[8] 周涛. 软计算与人工智能. 福建电脑,2006.1.

[9] [美]William Stallings. 密码编码学与网络安全. 张焕国等译. 北京：电子工业出版社, 2006.

[10] 薛锐,冯登国. 安全协议的形式化分析技术与方法. 计算机学报,2006,29(1):1-20.

[11] 张福泰等. 密码学教程. 武汉：武汉大学出版社,2006.

[12] 周永彬,冯登国. RFID 安全协议的设计与分析. 计算机学报,2006,29(4):581-589.

[13] 周琴. 计算机病毒研究与防治. 计算机与数字工程,2006,03:86-90.

[14] 赵育新,赵连凤. 计算机病毒的发展趋势与防治. 辽宁警专学报,2006,06:45-47.

[15] 韩权印,张玉清,聂晓伟. BS 7799 风险评估的评估方法设计. 计算机工程,2006,02:140-143.

[16] 魏亮. 网络与信息安全标准研究现状. 电信技术,2006,05:24-27.

[17] 周琴. 计算机病毒研究与防治. 计算机与数字工程,2006,03:86-90.

[18] 孙璇. WAPI 协议的分析及在 WLAN 集成认证平台中的实现. 西安电子科技大学,2006.

[19] 苏忠等. 无线传感器网络密钥管理的方案和协议. 软件学报,2007,18(5):1218-1231.

[20] 任秀丽,于海斌. ZigBee 无线通信协议实现技术的研究. 计算机工程与应用,2007(6):143-145.

[21] 游战清等. 无线射频识别系统安全指南. 北京：电子工业出版社,2007.11.

[22] 龙涛. 开放网格服务架构下的安全策略研究[D]. 华中科技大学,2007.

[23] 曹大元. 入侵检测技术. 北京：人民邮电出版社,2007.5.

[24] 裴庆祺等. 无线传感器网络安全技术综述. 通信学报,2007,Vol.28(8):113-122.

[25] 高长喜等. IEEE 802.16 安全机制的研究与实现. 无线电工程,2007,37(10):1-4.

[26] 潘晓,肖珍,孟小峰. 位置隐私研究综述. 计算机科学与探索,2007,1(3):268-281.

[27] 朱勤,骆轶姝,乐嘉锦. 数据库加密与密文数据查询技术综述. 东华大学学报(自然科学版),2007, Vol.33(4):543-548.

[28] 邓峰,张航. 计算机网络威胁与黑客攻击浅析. 网络安全技术与应用,2007,11:23-24.

[29] 曹莉兰. 基于防火墙技术的网络安全机制研究[D]. 电子科技大学,2007.

[30] 李声. 防火墙与入侵检测系统联动技术的研究与实现[D]. 南京航空航天大学,2007.

[31] 郭曙光. 信息安全评估标准研究与比较. 信息技术与标准化,2007,11:27-29.

[32] 朱方洲. 基于 BS 7799 的信息系统安全风险评估研究[D]. 合肥工业大学,2007.

[33] 李剑. 入侵检测技术. 北京：高等教育出版社,2008.

[34] 侯春萍,宋梅,蔡涛. 蓝牙核心技术. 北京：机械工业出版社,2008.

[35] 刘宗伟. IPv6 安全技术研究[D]. 吉林大学,2008.

[36] 关振胜. 公钥基础设施 PKI 及其应用. 北京：电子工业出版社,2008.

[37] 荆继武,林璟锵,冯登国. PKI 技术. 北京：科学出版社,2008.

[38] 郎为民. 射频识别(RFID)技术原理与应用. 北京：机械工业出版社,2008.

[39] 王晓华. RFID 系统的安全问题及其解决方案. 设施与设备,2008,Vol.27(1):110-116.

[40] 裘友林,杨善林. 基于密钥矩阵的 RFID 安全协议. 计算机工程,2008,Vol.34(19):170-173.

[41] 步山岳. 计算机信息安全技术. 北京：高等教育出版社,2009.
[42] 顾丽,王广泽,乔佩利. 基于改进遗传算法的入侵检测的研究. 信息技术,2009.
[43] 戴沁芸等. 浅析下一代移动通信网络的安全问题. 信息安全与通信保密,2009.9.
[44] Behrouz A. Forouzan. 密码学与网络安全. 马振晗,贾军保译. 北京：清华大学出版社,2009.
[45] 曹天杰,张永平,汪楚娇. 安全协议. 北京：北京邮电大学出版社,2009.
[46] 落红卫. 手机病毒及应对技术探究. 信息网络安全,2009(9).
[47] 张宝军. 网络入侵检测若干技术研究[D]. 浙江大学,2009.
[48] 周伟. 异构网络中的移动管理和安全机制研究[D]. 中国科学技术大学,2009.
[49] 孙立新,张栩之. 关于计算机网络系统物理安全研究与分析. 网络安全技术与应用,2009,10:67-68.
[50] 邓清华. 计算机病毒传播模型及防御策略研究[D]. 华中师范大学,2009.
[51] 刘扬. 防火墙安全策略管理系统设计与实现[D]. 国防科学技术大学,2009.
[52] 张磊. 安全网络构建中防火墙技术的研究与应用[D]. 山东大学,2009.
[53] 马利. 计算机信息安全技术. 北京：清华大学出版社,2010.
[54] 武传坤. 物联网安全机构初探. 中国科学院院刊,2010.5.
[55] 边瑞昭等. 3G 中安全增强的 AKA 协议设计与分析. 计算机应用与软件,2010.1.
[56] 李建华. 公钥基础设施(PKI)理论及应用. 北京：机械工业出版社,2010.3.
[57] 戴沁芸. 第三代移动通信系统网络接入安全机制分析. 现代电信科技,2010.4.
[58] 吴文玲等. 鲁班锁轻量级分组密码详细设计. 信息安全国家重点实验室技术报告,2010.
[59] 武传坤. 物联网安全架构初探. 战略与决策研究,2010,Vol.25(4):411-419.
[60] 杨庚等. 物联网安全特征与关键技术. 南京邮电大学学报,2010,Vol.30(4):20-29.
[61] 武传坤. 物联网安全机构初探. 中国科学院院刊,2010.5.
[62] 陈柳钦. 物联网国内外发展动态及亟待解决的关键问题. 决策咨询通讯,2010,(5):15-25.
[63] 洪帆. 访问控制概论. 武汉：华中科技大学出版社,2010.8.
[64] 宁焕生. RFID 重大工程与国家互联网. 北京：机械工业出版社,2010.9.
[65] 姜奇等. 基于 WAPI 的 WLAN 与 3G 网络安全融合. 计算机学报,2010.9.
[66] 王凤英. 访问控制原理与实践. 北京：北京邮电大学出版社,2010.12.
[67] 中国密码学会组. 中国密码学发展报告 2010. 北京：电子工业出版社,2011.
[68] 吴刚. 基于多 Agent 的物联网信息融合方法的研究[D]. 南京邮电大学,2011.
[69] 温蜜,邱卫东. 基于传感器网络的物联网密钥管理. 上海电力学院学报,2011.
[70] 周洪波. 物联网：技术、应用、标准和商业模式. 第 2 版. 北京：电子工业出版社,2011.
[71] 王杰. 计算机网络安全的理论与实践. 第 2 版. 北京：高等教育出版社,2011.
[72] 艾浩军等. 物联网：技术与产业发展. 北京：人民邮电出版社,2011.
[73] 彭春燕. 基于物联网的安全架构. 网络安全技术与应用. 2011,(5):13-14.
[74] 王汝林. 物联网基础及应用. 北京：清华大学出版社,2011.
[75] 李志清. 物联网安全问题研究. 网络安全技术与应用. 2011,(10):33-35.
[76] 刘海涛. 互联网之感知社会论. 上海：华东师范大学出版社,2011.
[77] 梁晨. 基于物联网的 RFID 安全认证协议研究与设计[D]. 西安电子科技大学,2011.
[78] 胡婕,宗平. 面向物联网的 RFID 安全策略研究. 计算机技术与发展,2011(5):151-154.
[79] 焦文娟. 物联网安全——认证技术研究[D]. 北京邮电大学,2011.
[80] 何明,江俊. 物联网技术及其安全性研究. 计算机安全,2011,(4):49-50.
[81] 雷吉成. 物联网安全技术. 北京：电子工业出版社,2012.
[82] 任伟. 物联网安全. 北京：清华大学出版社,2012.
[83] 杜芸芸等. 云计算安全问题综述. 网络安全技术与应用,2012,(8):12-14.
[84] 徐小涛,杨志红. 物联网信息安全. 北京：人民邮电出版社,2012.
[85] 李联宁. 物联网安全导论. 北京：清华大学出版社,2013.

[86] 武传坤. 物联网安全基础. 北京：科学出版社，2013.
[87] 于旭，梅文. 物联网信息安全. 西安：西安电子科技大学出版社，2014.
[88] 张凯. 物联网安全教程. 北京：清华大学出版社，2014.
[89] 赵贻竹，鲁宏伟. 物联网系统安全与应用. 北京：电子工业出版社，2014.
[90] 王金甫，施勇，王亮. 物联网安全. 北京：北京大学出版社，2014.
[91] 桂小林，张学军，赵建强. 物联网信息安全. 北京：机械工业出版社，2014.
[92] He Yeye, Barman S, Naughton J F. Preventing equivalence attacks in updated, anonymized data. 2011 IEEE 27th International Conference on Data Engineering (ICDE). Hannover, 2011:529-540.
[93] Y. Mo, T. H.-J. Kim, K. Brancik, et al. Cyber-Physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE, Vol. 100, no. 1, pp. 195-209, Jan, 2012.

图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用,本书提供配套的素材,有需求的用户请到清华大学出版社主页(http://www.tup.com.cn)上查询和下载,也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题,或者有相关图书出版计划,也请您发邮件告诉我们,以便我们更好地为您服务。

我们的联系方式:

地　　址:北京海淀区双清路学研大厦 A 座 707

邮　　编:100084

电　　话:010-62770175-4604

资源下载:http://www.tup.com.cn

电子邮件:weijj@tup.tsinghua.edu.cn

QQ:883604(请写明您的单位和姓名)

扫一扫

资源下载、样书申请

新书推荐、技术交流

用微信扫一扫右边的二维码,即可关注清华大学出版社公众号"书圈"。